Implementation of Web Application Firewall

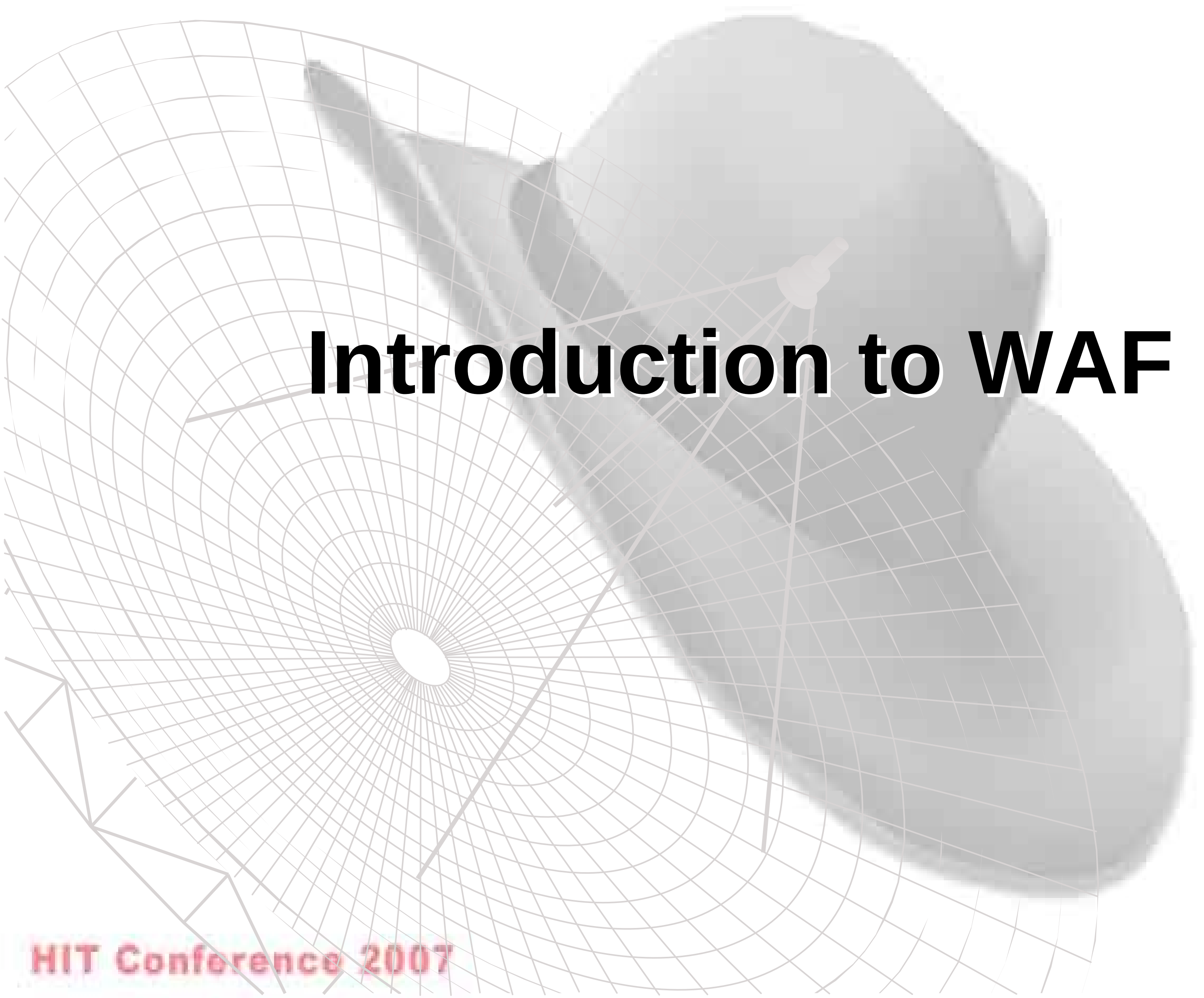
OuTian <outian@chroot.org>

Introduction

- **Abstract**
  - **Web** 層應用程式之攻擊日趨嚴重，而國內多數企業仍不知該如何以資安設備阻擋，仍在採購傳統的 **Firewall/IPS** ，因此本場次即對 **Web Application Firewall(** 以下簡稱 **WAF)**之功能、及實作方式作介紹
- **About OuTian**
  - 現任 敦陽科技 資安顧問
  - 滲透測試服務與後續資安規劃
  - 資安事件鑑識處理

Agenda

- Introduction to WAF
- General Web Vulnerabilities
- Functions
- Implementation
- Common Questions
- Evasion
- Conclusion
- Q & A



Introduction to WAF

Introduction to WAF

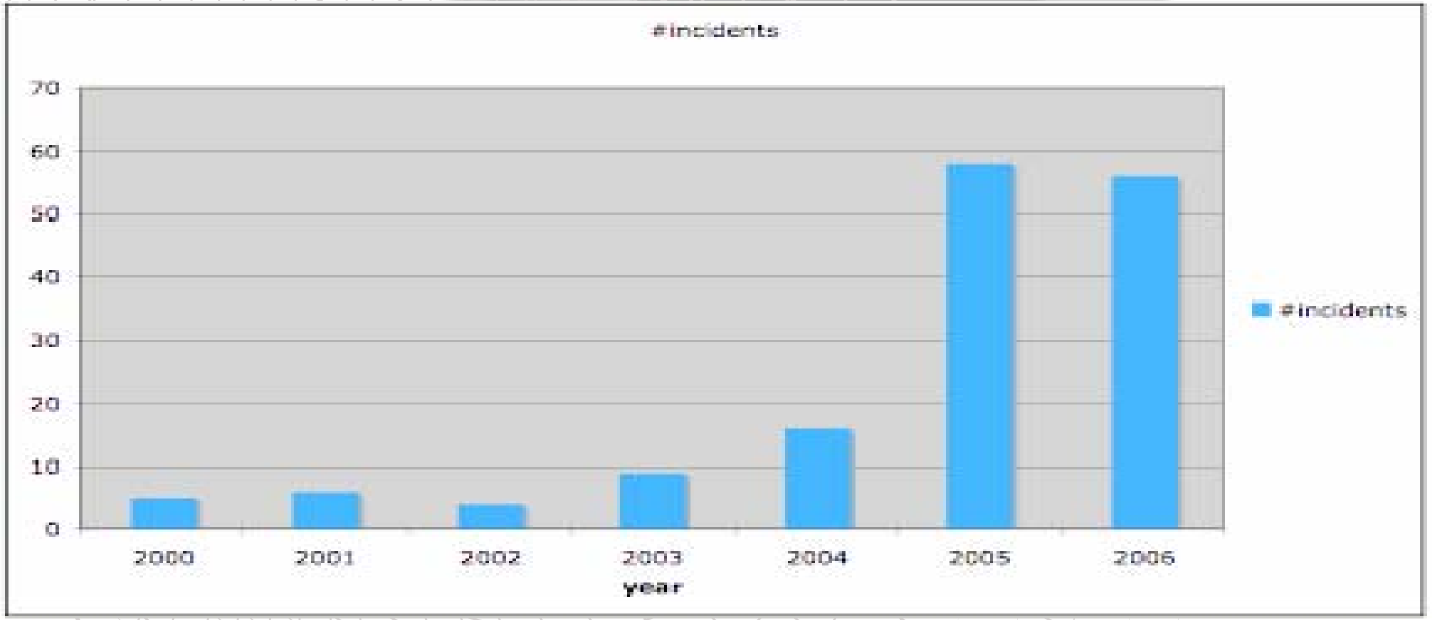
- What is WAF
- Why WAF
- Vendors
- Structure
- WAF v.s Network Firewall
- WAF v.s IPS

What is WAF

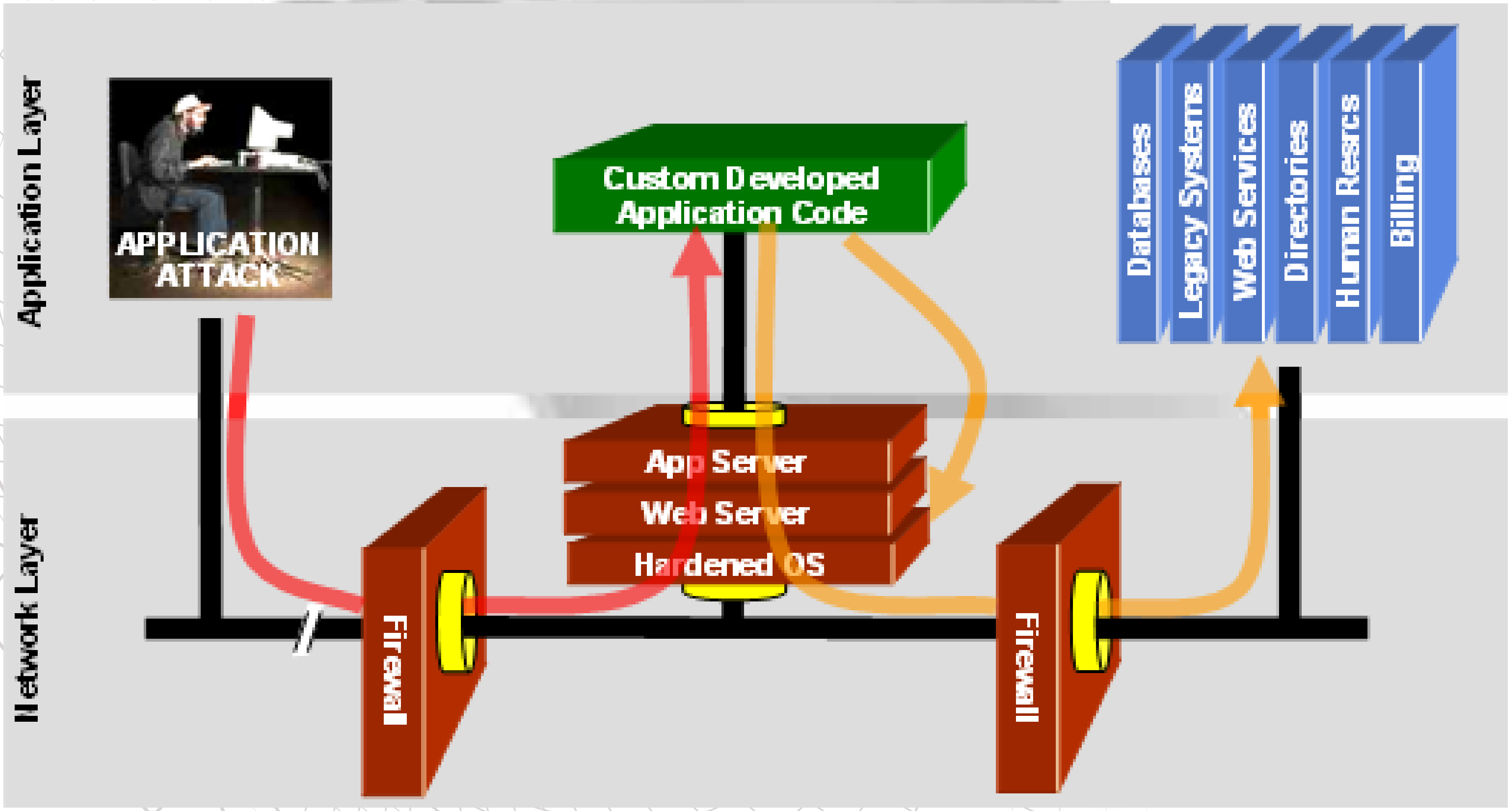
- An intermediary device, sitting between a web-client and a web server, analyzing OSI Layer-7 messages for violation in the programmed security policy. A web application firewall is used as a security device protecting the web server from attack.

Why WAF

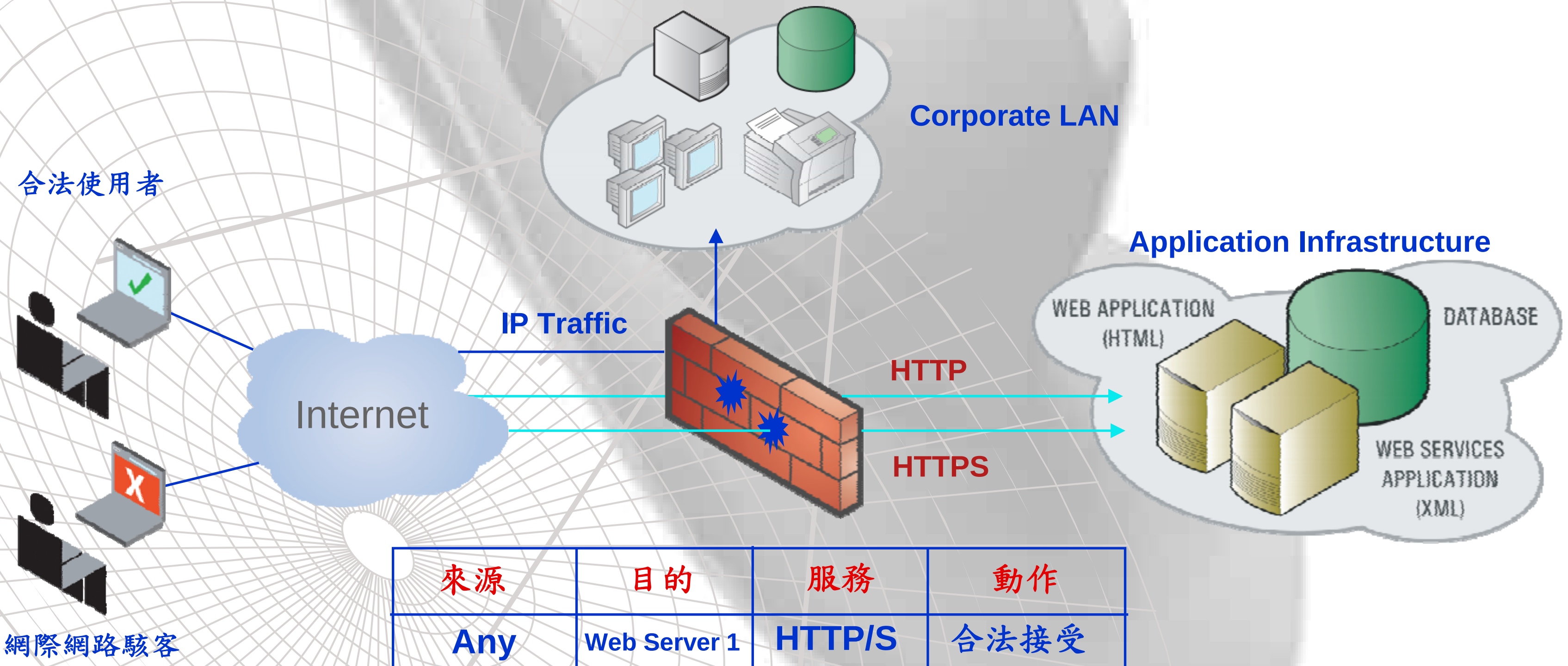
- **Web AP 成為 顧客/駭客 共同入口**
  - **根據Gartner統計：
    成功的惡意攻擊中，70% 都是針對 Web AP**



既有的資安設備無法有效阻擋



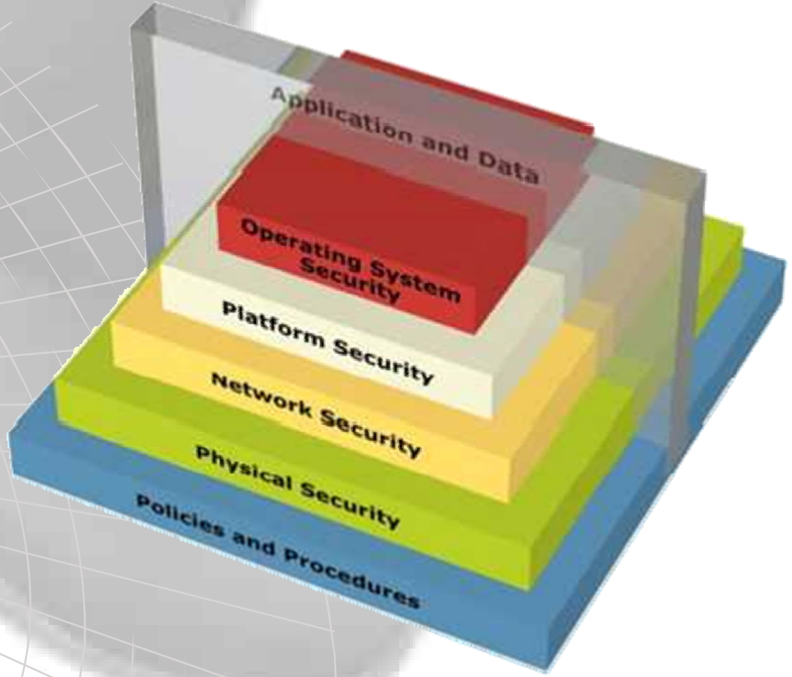
SSL 加密，IDS/IPS也看不懂



來源	目的	服務	動作
Any	Web Server 1	HTTP/S	合法接受

Web AP 安全來源的複雜性

- 複雜之 **AP Source Code**
- 開發者多數僅注重功能
- 類似的安全問題重複發生
- 其他引用來源所累



Vendors

- Breach
- Citrix
- F5
- Imperva
- NetContinuum
- WebScurity

Structure

- Host Based
  - Web Server module / plugin
  - Special program compiler
- Network Based
  - Appliance
  - Deployed as
    - Reverse Proxy
    - In-Line Mode
    - Web Traffic Monitor
  - SSL Handshaking

WAF v.s Network Firewall

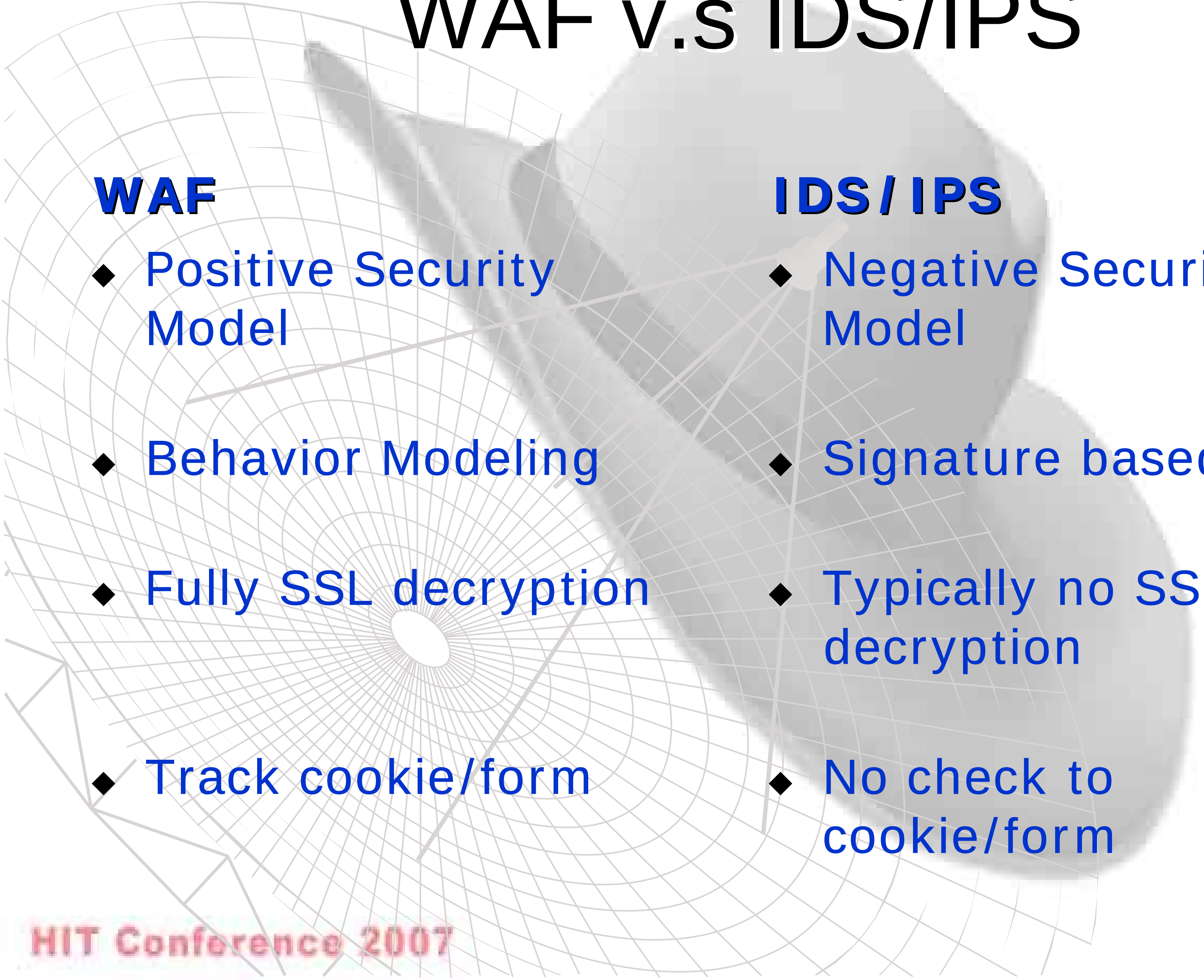
WAF

- Protect at Layer 7
- Check http/s data
- Block http/s traffic with malicious attack
- Decrypt https packets
- Inspect http/html

Network Firewall

- Protect at Layer 3
- check IP and PORT
- Always allow http/s traffic even with malicious attack
- Unable to decrypt https packet
- No action to http/html

WAF v.s IDS/IPS



WAF	**IDS / IPS**
◆ Positive Security Model	◆ Negative Security Model
◆ Behavior Modeling	◆ Signature based
◆ Fully SSL decryption	◆ Typically no SSL decryption
◆ Track cookie/form	◆ No check to cookie/form

General Web Vulnerabilities

General Web Vulnerabilities

- **Web Application Design Error**
  - **Buffer Overflow**
  - **SQL Injection**
  - **Cross Site Scripting**
  - **Arbitrary File Inclusion**
  - **Code Injection**
  - **Command Injection**
  - **Directory Traversal**

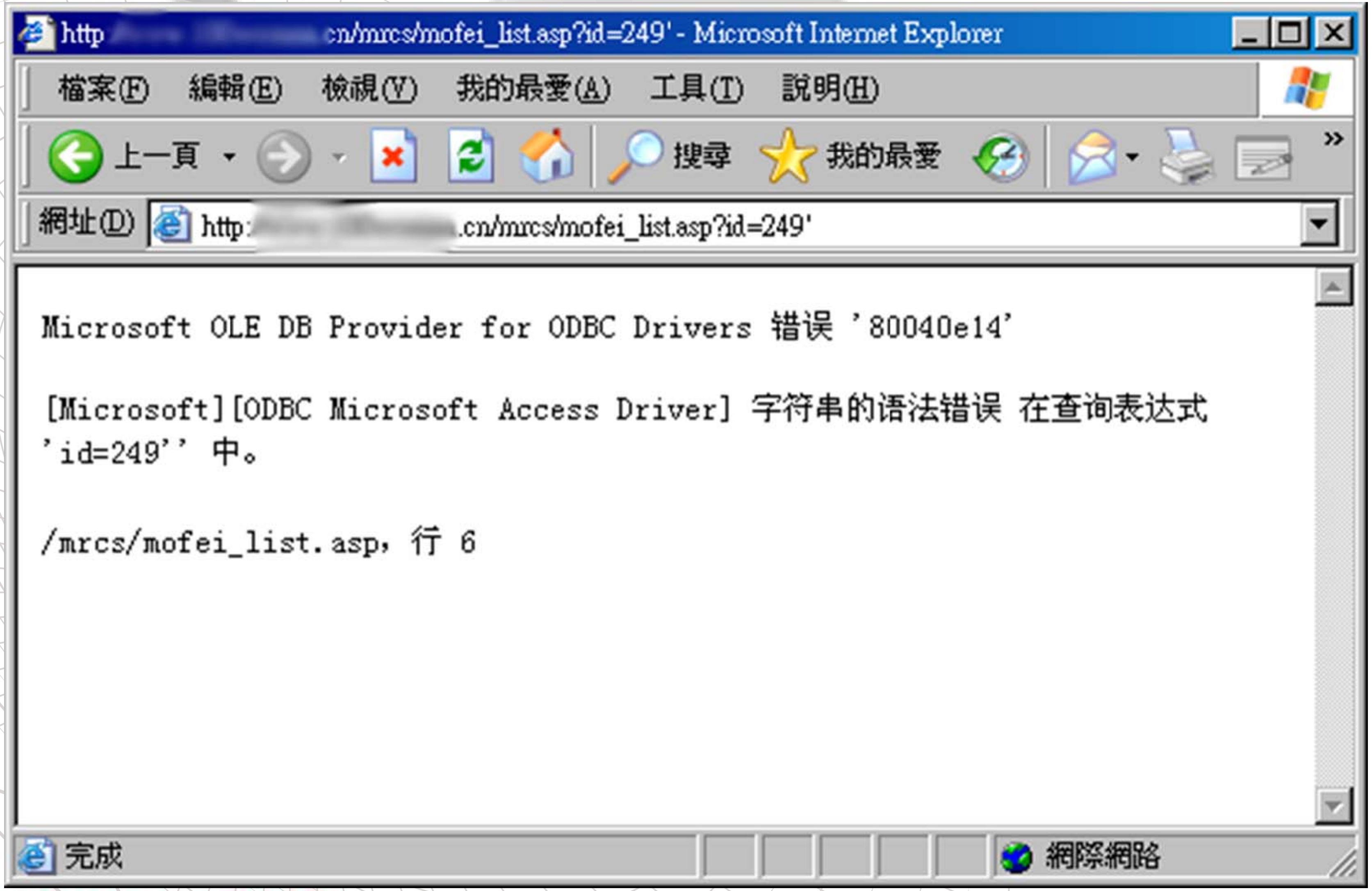
- Logic Design Error
  - Cookie Poisoning
  - Parameter Tampering
  - Session Mis-Management
  - Upload File Mis-Handling
  - Information Disclosure
  - Weak Authentication

OWASP top 10 2007

- Cross Site Scripting
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery

- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access

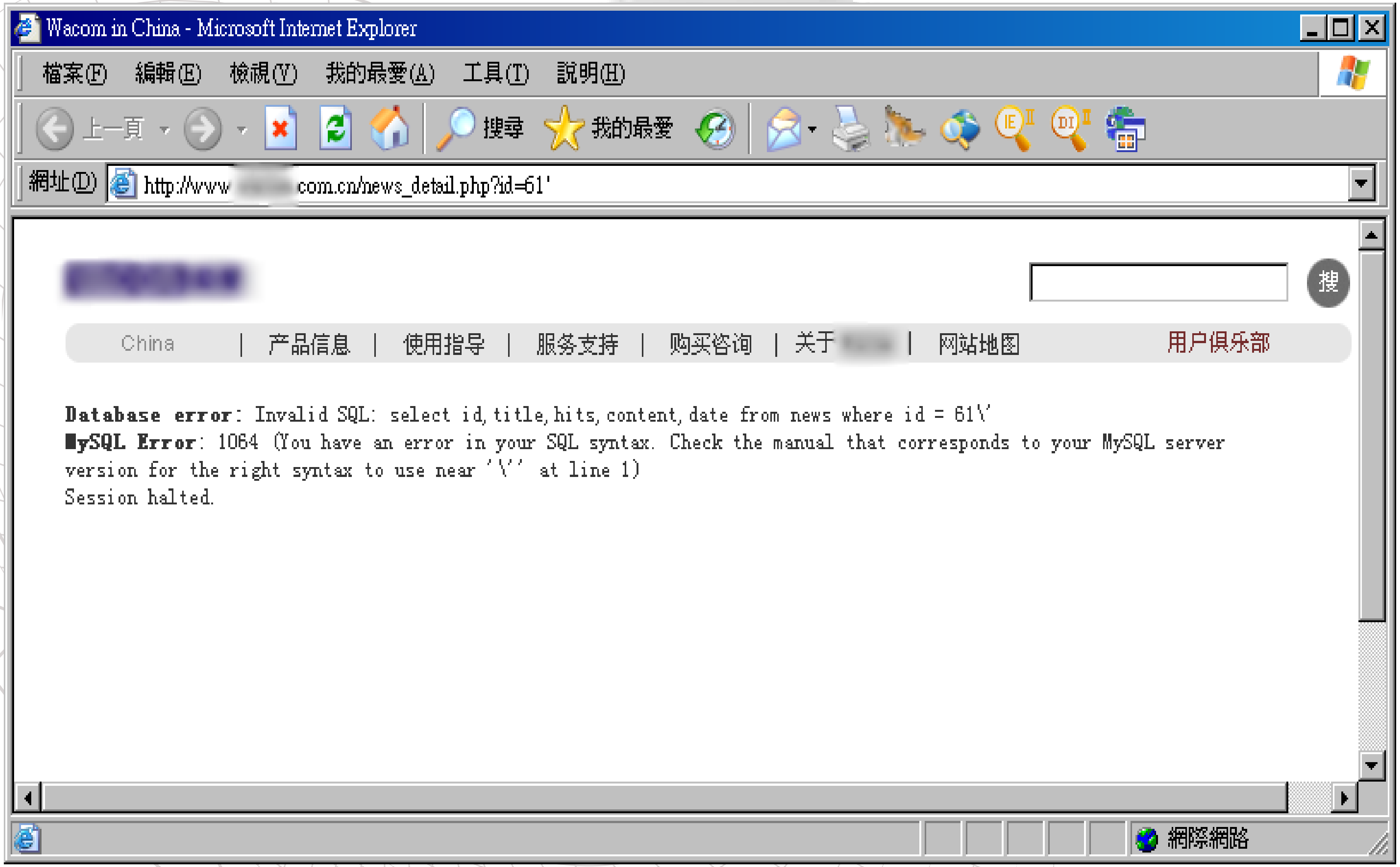
SQL Injection Example


http [redacted] cn/mrcs/mofei_list.asp?id=249' - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
http: [redacted] .cn/mrcs/mofei_list.asp?id=249'
完成
網際網路

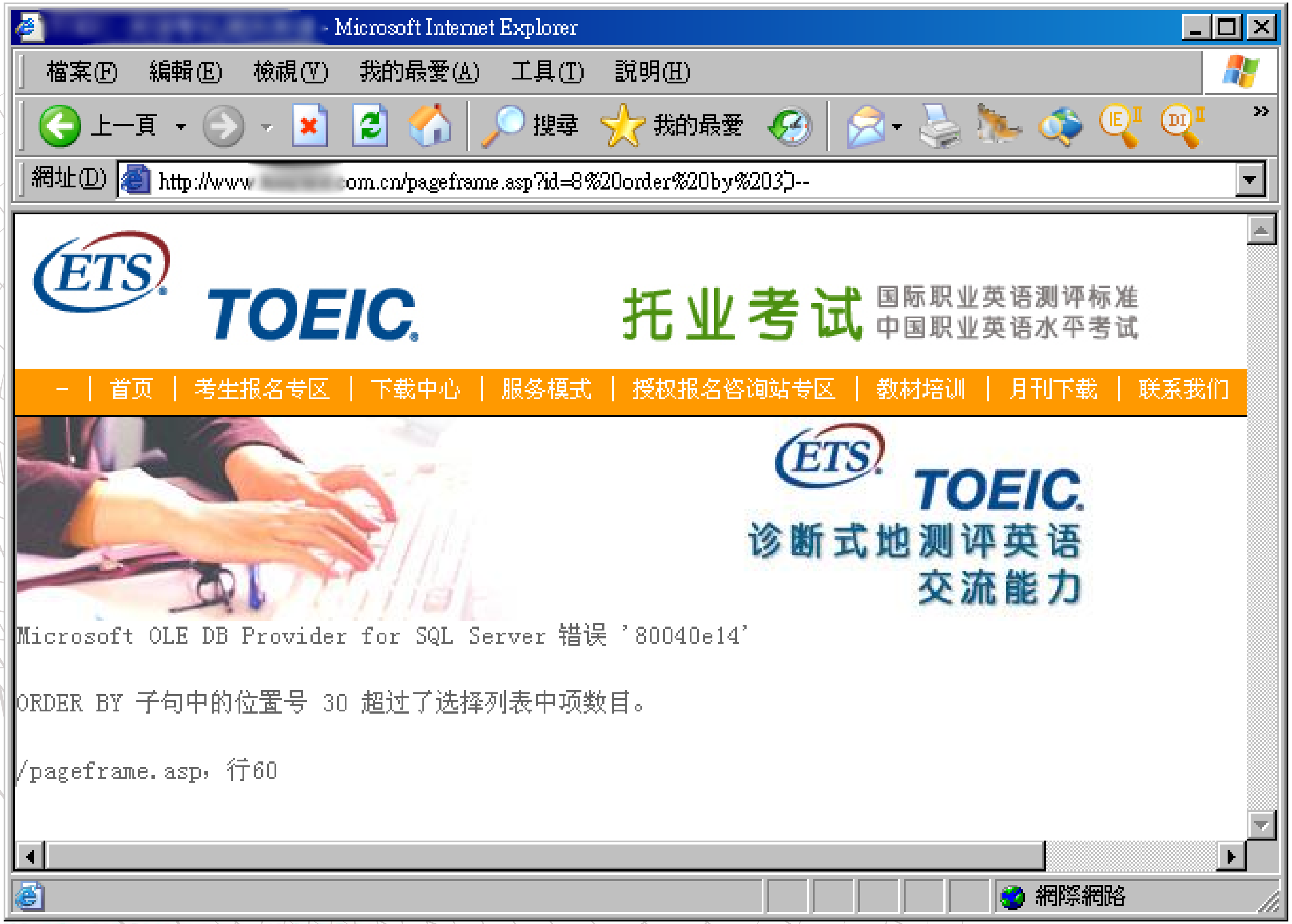
```
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e14'

[Microsoft][ODBC Microsoft Access Driver] 字符串的语法错误 在查询表达式
'id=249'' 中。

/mrcs/mofei_list.asp, 行 6
```


Wacom in China - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
http://www.[redacted]com.cn/news_detail.php?id=61'
搜
China | 产品信息 | 使用指导 | 服务支持 | 购买咨询 | 关于[redacted] | 网站地图 用户俱乐部
網際網路

```
Database error: Invalid SQL: select id,title,hits,content,date from news where id = 61\'
MySQL Error: 1064 (You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server
version for the right syntax to use near '\'' at line 1)
Session halted.
```


[redacted] - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D)
ETS
TOEIC
托业考试
国际职业英语测评标准
中国职业英语水平考试
首页 | 考生报名专区 | 下载中心 | 服务模式 | 授权报名咨询站专区 | 教材培训 | 月刊下载 | 联系我们
诊断式地测评英语交流能力
網際網路

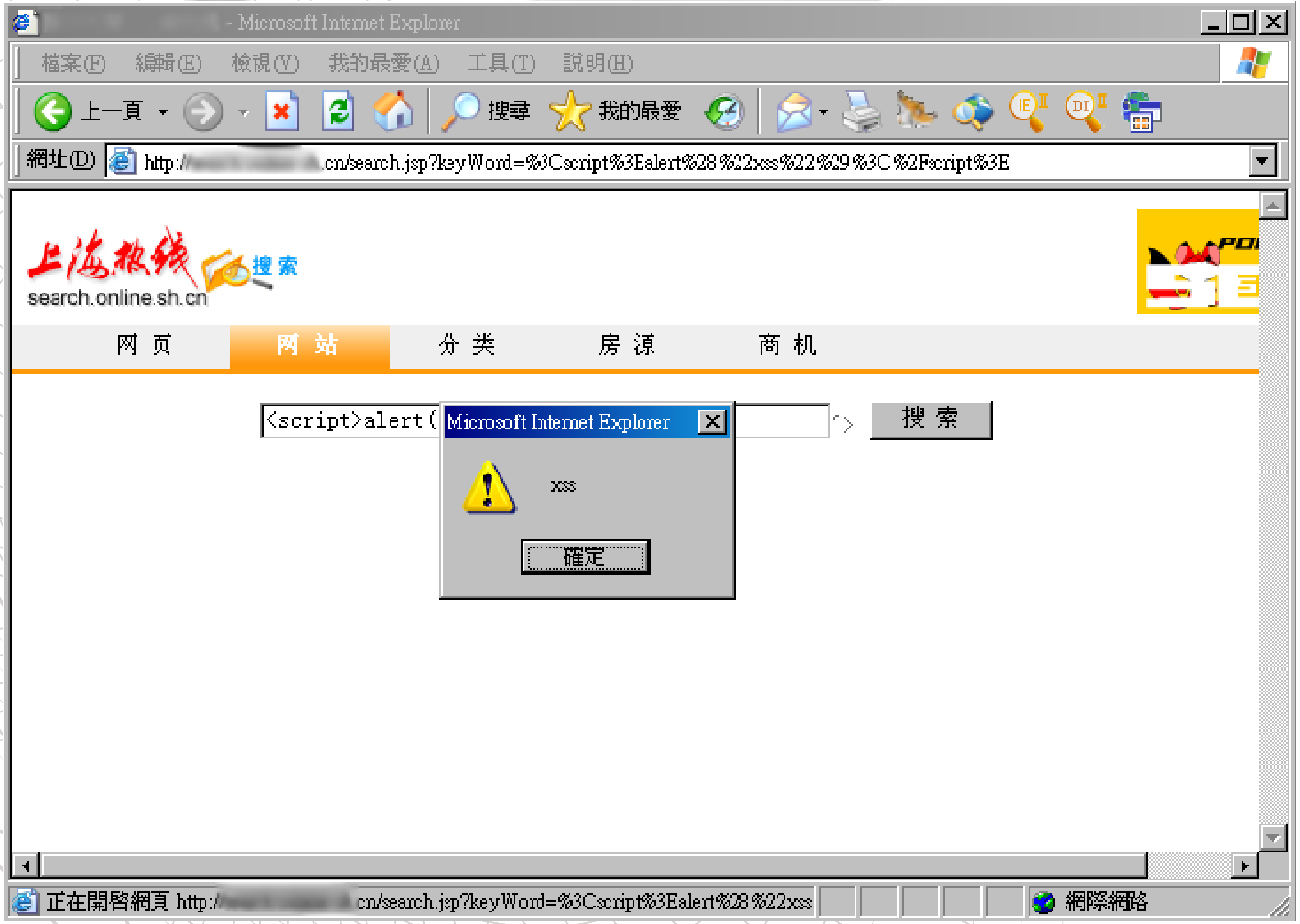
```
http://www[redacted]om.cn/pageframe.asp?id=8%20order%20by%2030--
```

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e14'

ORDER BY 子句中的位置号 30 超过了选择列表中项数目。

/pageframe.asp，行60
```

Cross Site Scripting Example



[redacted] - Microsoft Internet Explorer

```
http://[redacted].cn/search.jsp?keyWord=%3Cscript%3Ealert%28%22xss%22%29%3C%2Fscript%3E
```

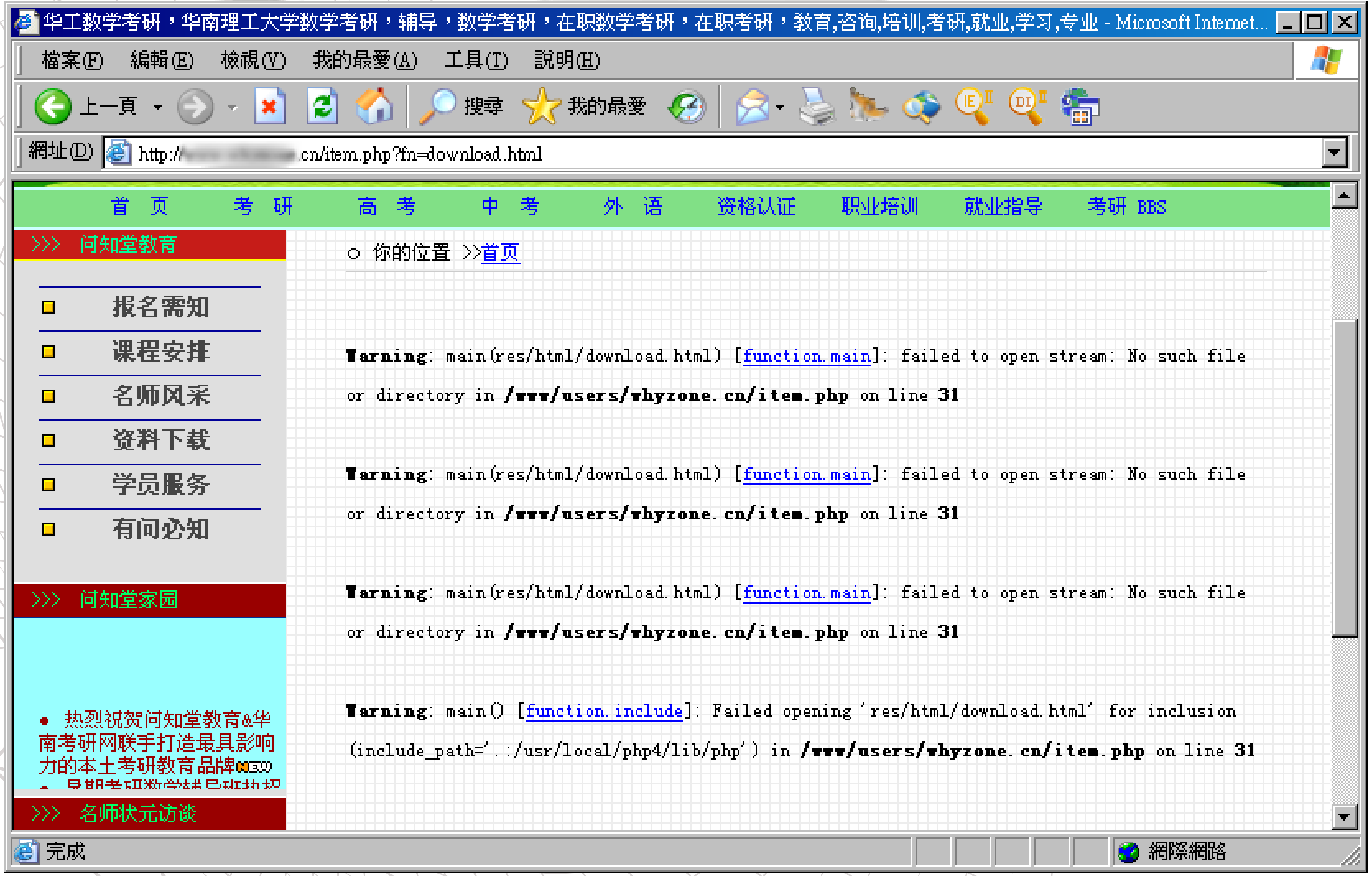
```
<script>alert(
```

Microsoft Internet Explorer

xss

```
正在開啓網頁 http://[redacted].cn/search.jsp?keyWord=%3Cscript%3Ealert%28%22xss
```

Arbitrary File Inclusion Example


华工数学考研，华南理工大学数学考研，辅导，数学考研，在职数学考研，在职考研，教育,咨询,培训,考研,就业,学习,专业 - Microsoft Internet...
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://[redacted]cn/item.php?fn=download.html
首 页 考 研 高 考 中 考 外 语 资格认证 职业培训 就业指导 考研 BBS
>>> 问知堂教育
报名需知
课程安排
名师风采
资料下载
学员服务
有问必知
>>> 问知堂家园
热烈祝贺问知堂教育&华南考研网联手打造最具影响力的本土考研教育品牌NEW
>>> 名师状元访谈
你的位置 >>首页
完成
網際網路

```
Warning: main(res/html/download.html) [function.main]: failed to open stream: No such file
or directory in /www/users/whyzone.cn/item.php on line 31

Warning: main(res/html/download.html) [function.main]: failed to open stream: No such file
or directory in /www/users/whyzone.cn/item.php on line 31

Warning: main(res/html/download.html) [function.main]: failed to open stream: No such file
or directory in /www/users/whyzone.cn/item.php on line 31

Warning: main() [function.include]: Failed opening 'res/html/download.html' for inclusion
(include_path='.:/usr/local/php4/lib/php') in /www/users/whyzone.cn/item.php on line 31
```

Functions

Functions

- **Input Validation**
  - **URL**
  - **Buffer Overflow**
  - **Form Field Consistency**
  - **Form Field Format**
  - **Cookie Consistency**
  - **SQL Injection**
  - **Cross Site Scripting**
- **Output Checks**

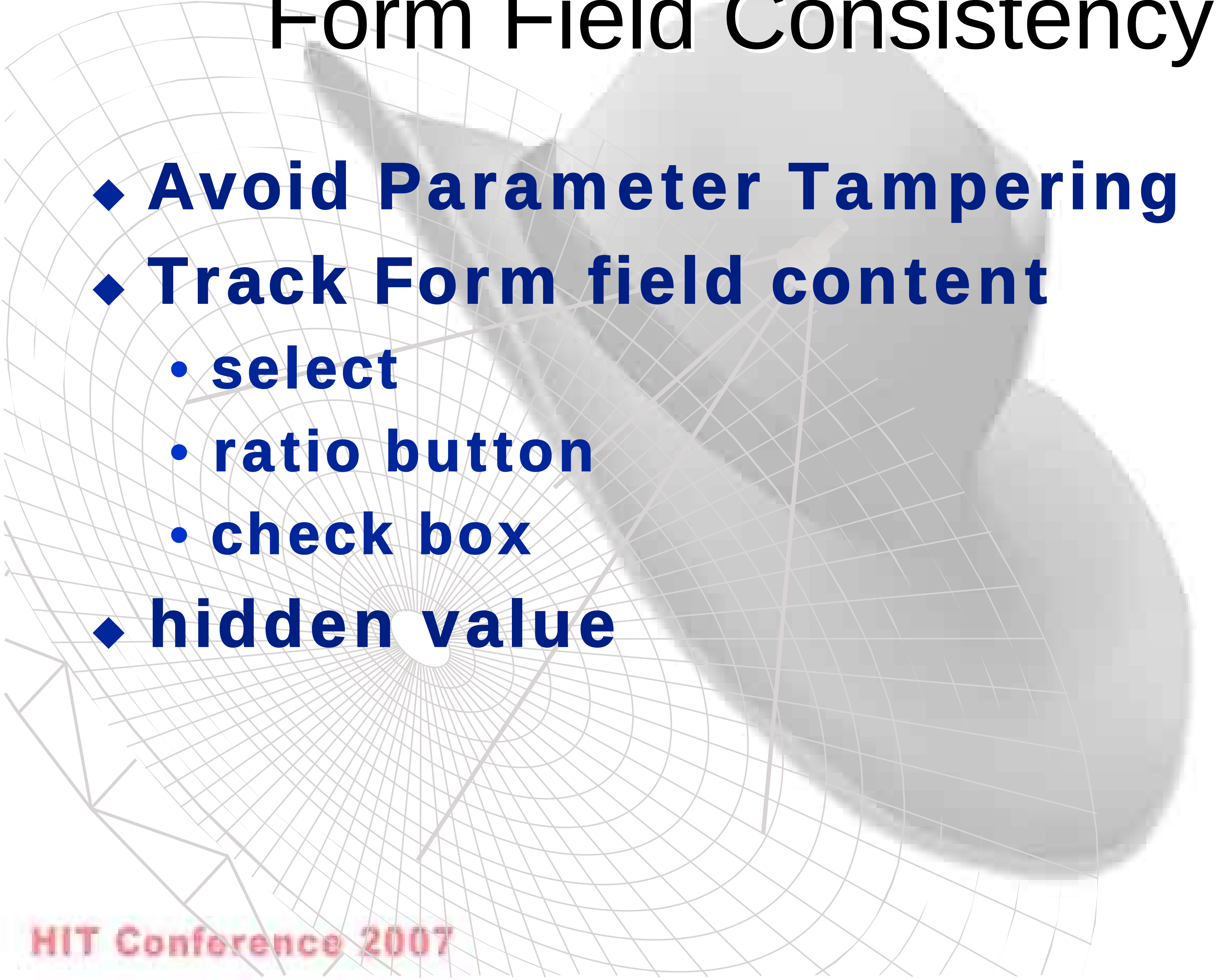
URL

- Check Allowed URL Resource
- Deny some file extensions
  - .phps
  - .inc
  - .sql
  - .core
  - .exe
  - .log

Buffer Overflow

- Limit maximum length of data
  - URL
  - Headers
  - Cookie
  - POST parameter
  - POST data

Form Field Consistency



- **Avoid Parameter Tampering**
- **Track Form field content**
  - **select**
  - **ratio button**
  - **check box**
- **hidden value**

Cookie Consistency

- Avoid Cookie Poisoning
- When web server Set-Cookie to client, WAF will track it to determine if modified by attacker

Field Format

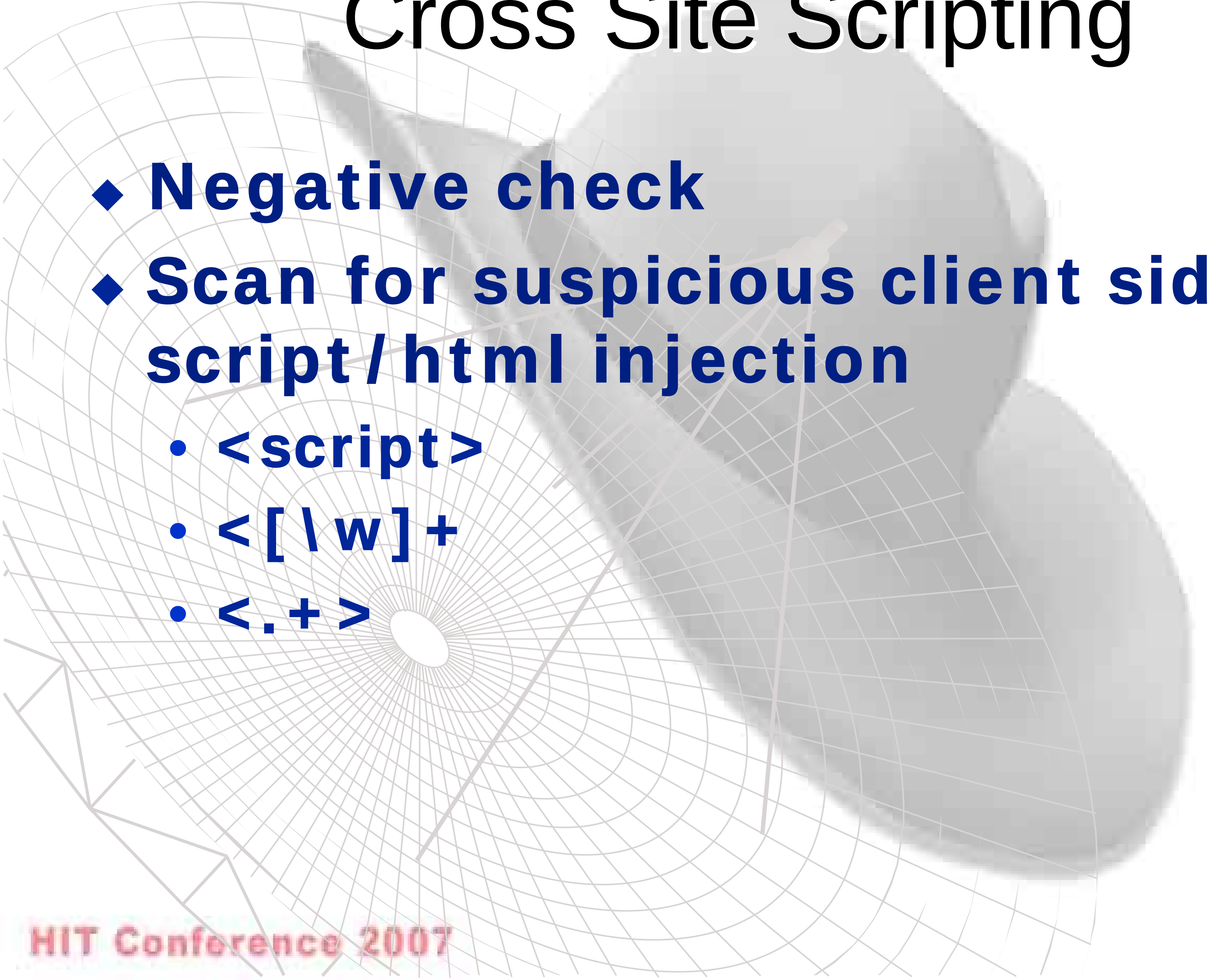
- User Input : GET / POST / Headers / Cookie
- Most effective way to avoid injection !
- Positive check
- Use Regular Expression to limit
  - uid => ^[0-9]+$
  - username => ^[\w\d]$
  - id => ^\w[0-9]{9}$

SQL Injection

- Negative check
- Scan for suspicious SQL character or SQL syntax
  - ‘
  - select / delete / update / insert
  - union / where / having / group
  - exec
  - --
  - / *

Cross Site Scripting

- Negative check
- Scan for suspicious client side script/html injection
  - <script>
  - <[\w]+
  - <.+>



Implementation

Implementation

- Apache
- Mod_security
- Mod_proxy
  - mod_proxy_http
  - mod_proxy_connect
  - mod_proxy_balancer
  - mod_proxy_ajp
- Mod_cache

Mod_security

- Open Source project : http://www.modsecurity.org/
- Embedded in apache web server
- Inexpensive and easy to deploy since no change to the network
- But must install/config to each web server

Features (1)

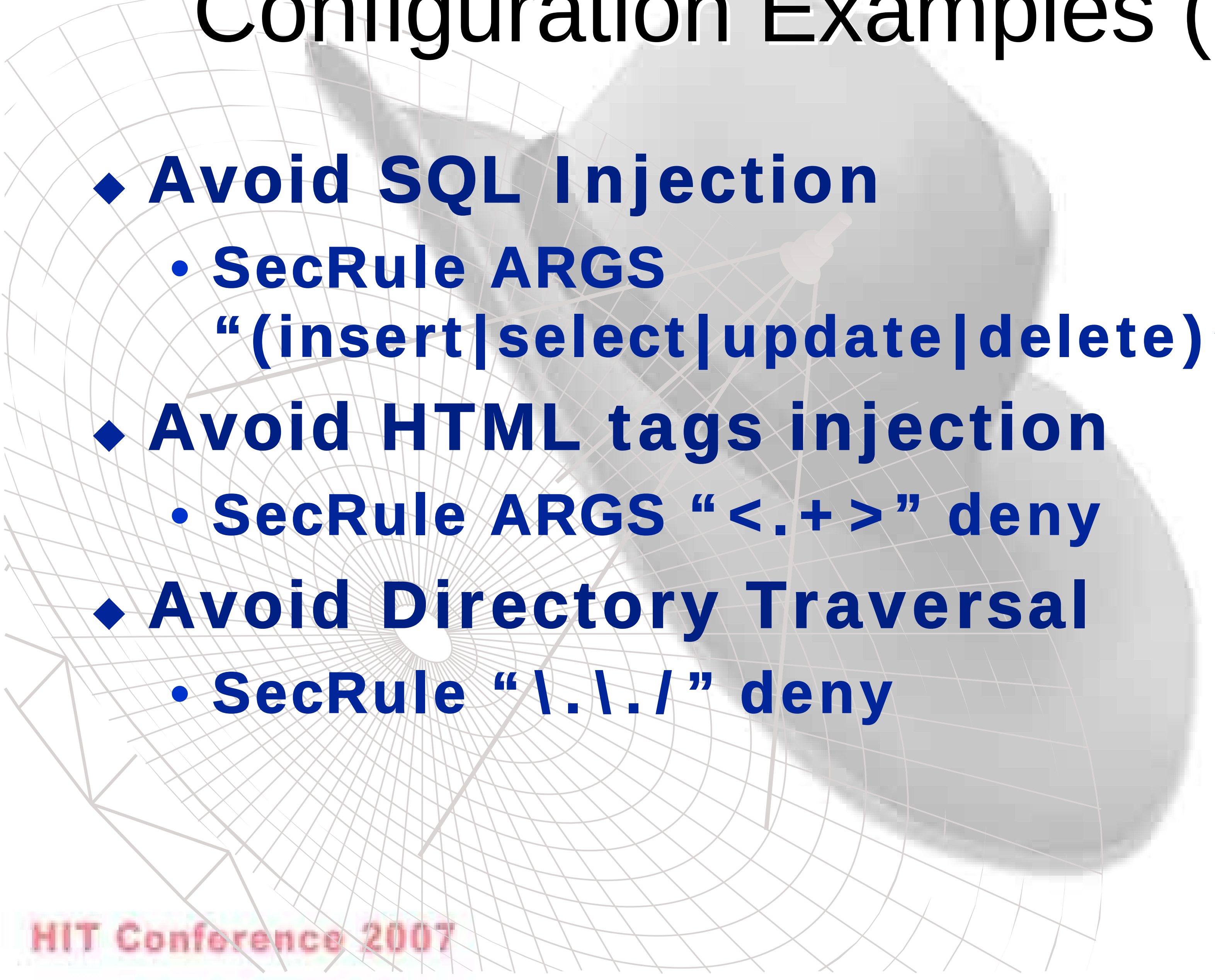
- Input validation check for all client input data
- Output check also available
- Buffer overflow protection
- Flexible
  - Regular Expression based rule engine
  - Different apps with different policies

Features (2)

- Anti-Evasion built in
- Upload file interception and real-time validation
- Encoding validation built in
- Up on attack detection, variety action to do : Log / Alert / Block / ...call scripts

Basic configuration concept

- **WHEN**
  - **found matched url / header / client / time**
- **DO**
  - **Check data**
- **THEN**
  - **Deny / pass / redirect / exec / ...**
- **Chain Rules**



Configuration Examples (1)

- **Avoid SQL Injection**
  - **SecRule ARGS "(insert|select|update|delete)" deny**
- **Avoid HTML tags injection**
  - **SecRule ARGS "<.+>" deny**
- **Avoid Directory Traversal**
  - **SecRule "\.\./" deny**

Configuration Examples (2)

- **Limit Login ip for admin**
  - **SecRule ARG_username "^admin$" chain**
  - **SecRule REMOTE_ADDR "!^192.168.0.1$" deny**
- **Hide Server Signature**
  - **SecServerSignature "MyWeb/1.0"**

Configuration Example (3)

- Avoid output credit card number
  - SecRule OUTPUT "\d{4}-\d{4}-\d{4}-\d{4}" "deny,phase:4"
- Avoid output php error message
  - SecRule OUTPUT "Warning:" "deny,phase:4,exec:mailadm.pl"
- Avoid output asp error message
  - SecRule OUTPUT "ODBC Drivers" "deny,phase:4,exec:mailadmin.pl"

Configuration Example (4)

- **chroot apache**
  - **SecChrootDir /chroot/apache**
- **Buffer overflow protection**
  - **SecFilterByteRange 32 126**

Mod_proxy

- **Mod_proxy_http**
  - **Proxy http request**
- **Mod_proxy_connect**
  - **Handel CONNECT http method**
- **Mod_proxy_balencer**
  - **Load sharing for server farms**
- **Mod_proxy_ajp**
  - **Support for apache jserv protocol**
- **Mod_proxy_ftp**
  - **Support proxying ftp sites**

Mod_cache

- **Mod_file_cache**
  - **Offers file handle and memory mapping tricks to reduce server load**
- **Mod_disk_cache**
  - **Implement disk based cache, content is stored in and retrived from the cache using URI based keys**
- **Mod_mem_cache**
  - **Caching open file descriptors and caching objects in heap storage**

Common Questions

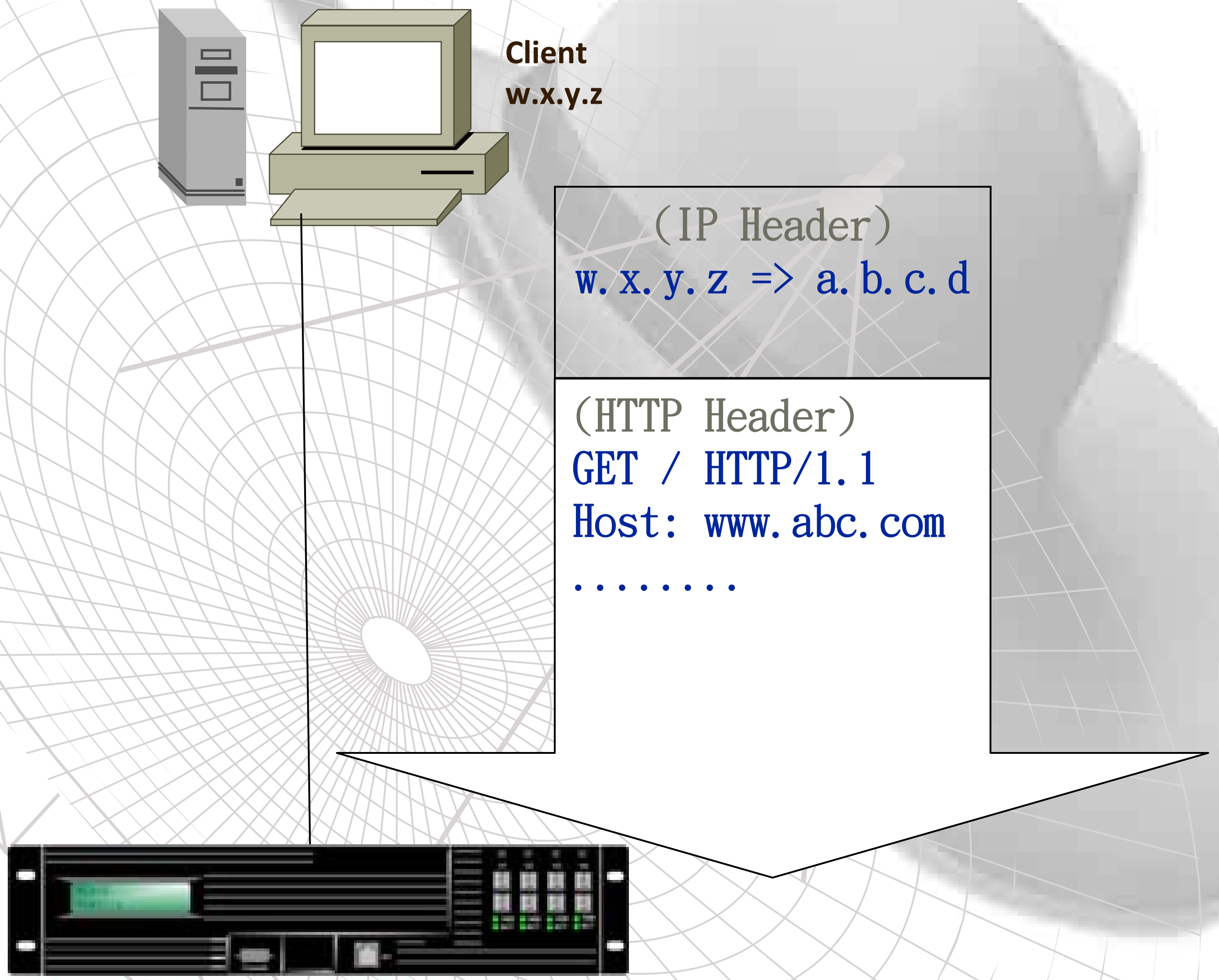
Common Questions

- **To see real client IP in Web AP and server logs**
- **L4 Devices sticky client by source ip**

To see real client IP (1)

- Environment –
  - Client ip : w.x.y.z
  - WAF external ip : a.b.c.d
  - WAF internal ip : 192.168.0.254
  - Web server ip : 192.168.0.1
  - Domain name : www.abc.com => a.b.c.d

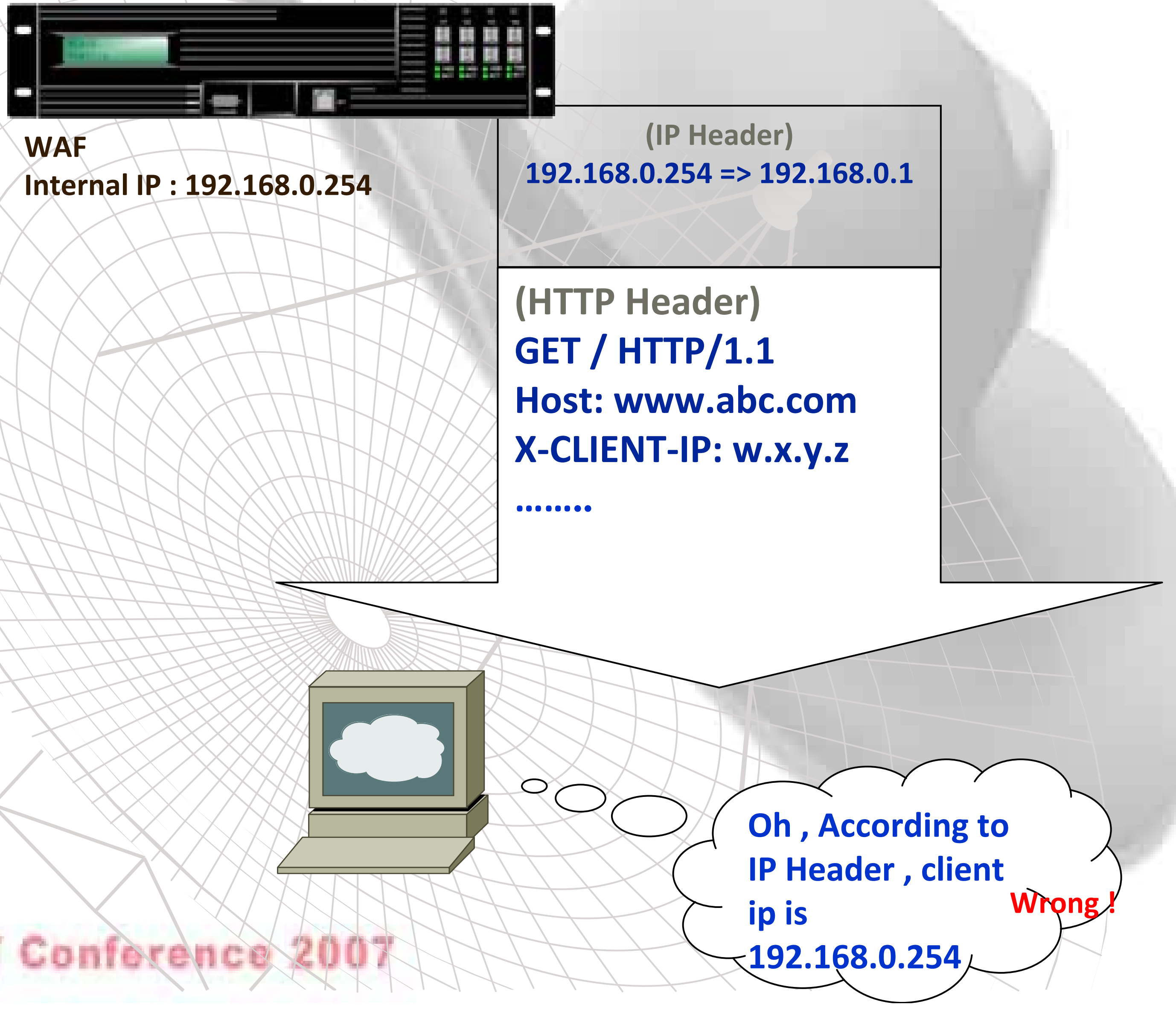
To see real client IP (2)



(IP Header)
w.x.y.z => a.b.c.d

(HTTP Header)
GET / HTTP/1.1
Host: www.abc.com
....

To see real IP (3)



To see real IP - solution

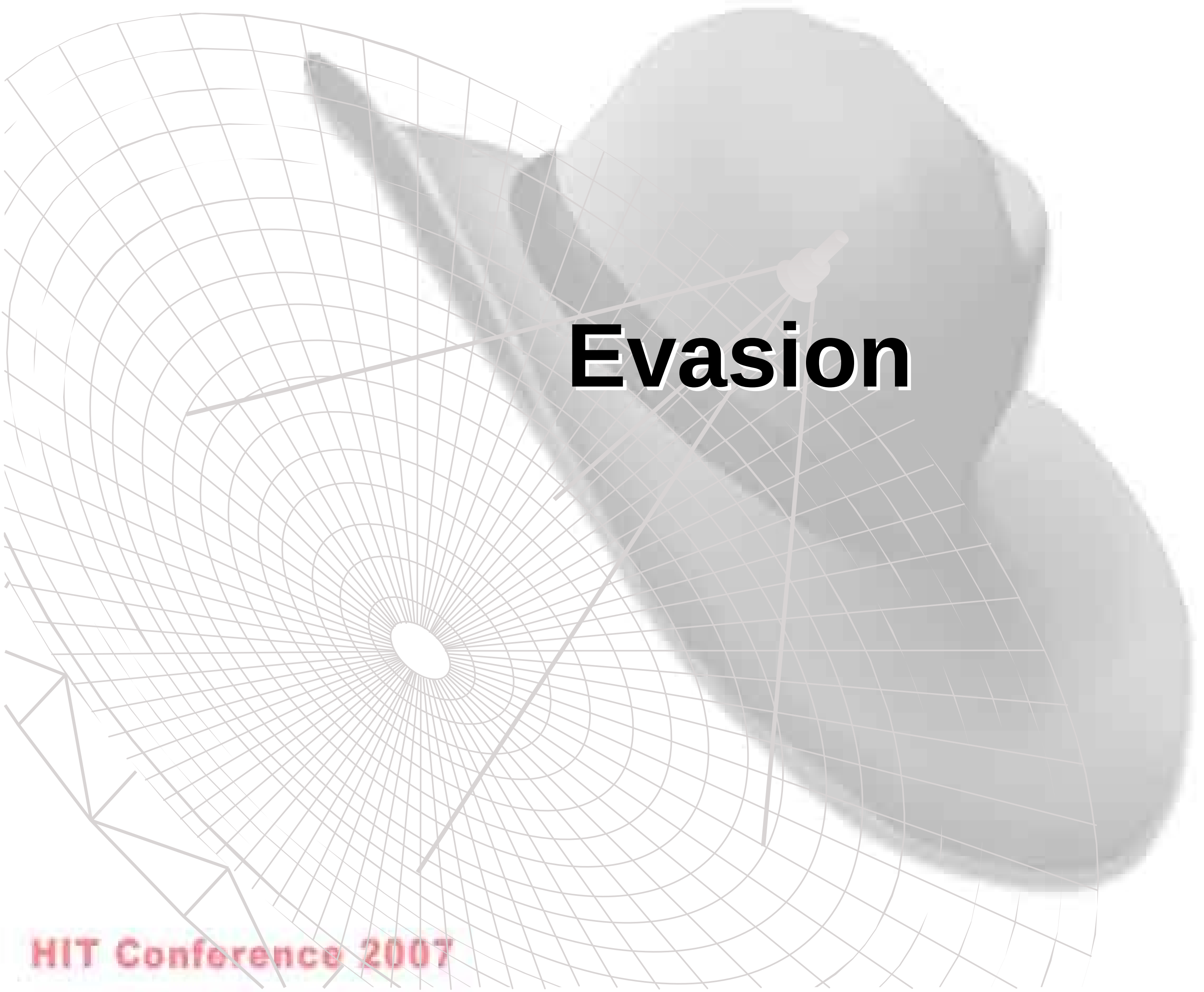
- **Web AP :**
  - **Rewrite to fetch real ip from http header**
- **Web Server Logs :**
  - **Apache – LogFormat / module**
  - **Tomcat – log pattern**
  - **IIS – IIS Filter**

Sticky client

- In most web AP, if web servers keep data in sessions on local disk, L4 devices must “sticky” the client in the same server, or the session may not be found.
- After deploying the WAF as reverse proxy, all source will from WAF, and make all clients sticky into the same servers, then make it overloaded.

Sticky client - solution

- **Set L4 Devices to sticky client by recognizing other data instead of source ip**
  - **Ex: Cookie -**
    - **PHPSESSID**
    - **JSESSIONID**
    - **ASPSSSID**
- **Set L4 to insert another cookie for sticky**



Evasion

Evasion

- **Simple Evasion Technique**
- **Path Obfuscation**
- **URL Encoding**
- **Unicode Encoding**
- **Null-Byte Attacks**

Simple Evasion Technique

- **Using mixed characters**
  - **In Microsoft Windows ,**
    test.asp == TEST.ASP
- **Character escaping**
  - **In some case ,**
    a = \a
- **Using whitespace**
  - **In SQL ,**
    delete from == delete   from

Path Obfuscation

- **Self-referencing directories**
  - **/test.asp == /./test.asp**
- **Double slashes**
  - **/test.asp == //test.asp**
- **Path traversal**
  - **/etc/passwd == /etc/./passwd**
  - **/etc/passwd == /etc/xx/../passwd**
- **Windows folder separator**
  - **../../cmd.exe == ..\..\cmd.exe**

URL Encoding

- **Path Encoding**
  - **/test.asp ==**
    /%74%65%73%74%2E%61%73%70
- **Parameter Encoding**
  - **?file=/etc/passwd**
    ==
    ?file=%2F%65%74%63%2F%70%61%73%73%77%64

Unicode Encoding

- **Overlong characters**

```
        0xc0 0x8A
     == 0xe0 0x80 0x8A
     == 0xf0 0x80 0x80 0x8A
     == 0xf8 0x80 0x80 0x80 0x8A
```

- **Unicode Encoding**

```
        /test.cgi?foo=../../bin/ls
     == /test.cgi?foo=..%2F../bin/ls
     == /test.cgi? foo=..%c0%af../bin/ls
```

Null-Byte Attacks

- Null Byte (0x00) is used for string termination
- Some checks stop when found null byte
- Ex: to evade /etc/passwd check
  - /test.asp?cmd=ls%00cat%20/etc/passwd

Conclusion

Conclusion

- In general, Web Application Firewall is the most effective solution for defending web attacks, but the most important of all – you must have enough knowledge to set up it correctly !
- It's complex to config it well, but we must do it !

- Open Source WAF solution is much cheaper than commercial devices, but you must control everything by yourself.
- Nothing could guarantee 100% perfect protection !

DEMO

Q & A