

가

가

1.

가
가

— — — — —

(.php, .jsp, .asp, .cgi, .pl) 가

가
가가
가

2.

```
- [ ] -> [ ] ->
[ ] -> [ ]
[ , ] -> [ ]
,
- httpd.conf
```

3. WebDAV

가 WebDAV

- NCSC(www.ncsc.go.kr) ‘ ,

httpext.dll Everyone

- /windows/system32/inetsrv/httpext.dll
Everyone

- []=>[] []
[]
[] [] ‘ ,

4. SQL Injection

DB , (‘ “ ” /
| ; : Space -- +),
SQL Injection

<http://www.sans.org/rr/whitepapers/securecode/23.php>

5. DB bak

.bak text

DB

Apache

- (admin) IP 가
httpd.conf Directory
AllowOverride AuthConfig All
가 .
- Apache httpd.conf

```
<Directory "/usr/local/www/admin/">  
  Order allow,deny  
  Deny from all  
  allow from 192.168.1.11 <-- 192.168.1.11 가  
</Directory>
```

- .htaccess : .htaccess
(AccessFile
Name .MyConfig) , httpd.conf AllowOverride
None Indexes ()

8.

- 가

```
- Apache httpd.conf -  
  <Directory "/usr/local/www">  
    Options Indexes <--  
  </Directory>  
  
  <Directory "/usr/local/www">  
    Options IFollowSymLinks <--  
  </Directory>
```

- []->[] [] ,]
-

9.

- ()
- ()
- include
- php.ini "allow_url_fopen = Off "
- "register_globals = Off "

XSS

- \$dir, \$_zb_path , preg_replac
- quotes
- http://www.nzeo.com/

10.

SSH brute force

WebDAV

가

.

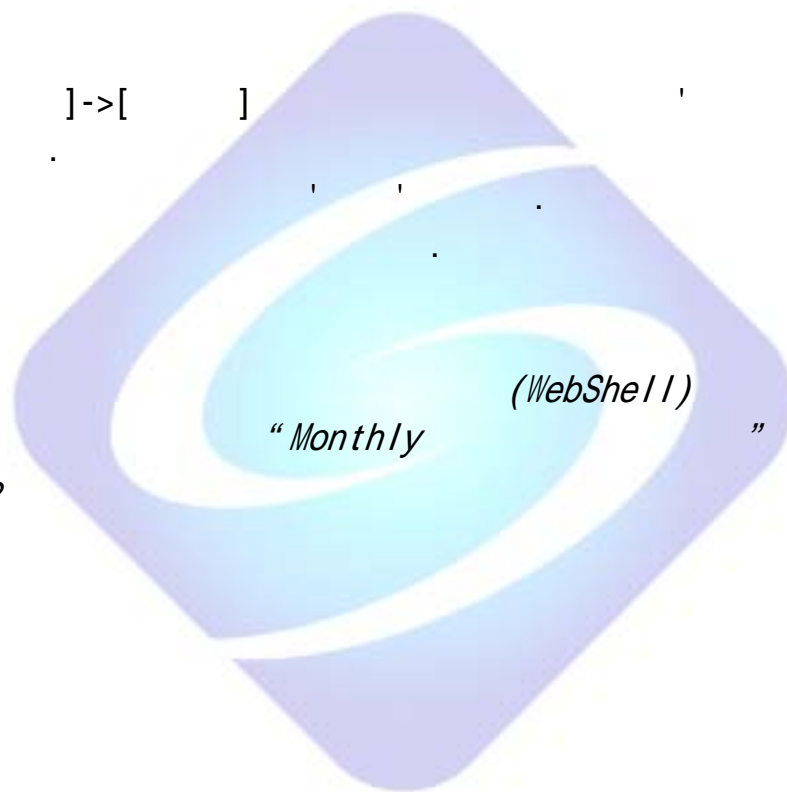
XP SP2

2003 SP1

- []->[]

-
-

1•2



“Monthly

(WebShell)

” ‘ 06