DVWA

20 June 2017, 10:29 AM

\seval\s*\(

ID: 37

warn

/home/chris/src/DVWA-master/dvwa/js/dvwaPage.js:6

```
 1:   /* Help popup */
 2:
 3:   function popUp(URL) {
 4:      day = new Date();
 5:      id = day.getTime();
 6:      eval("page" + id + " = window.open(URL, '" + id + "', 'toolbar=0,scrollbars=1,location=0,statusbar=0,menubar=0,resizable=1,
 7:   }
 8:
 9:   /* Form validation */
10:
11:    function validate_required(field,alerttxt)
```

Questionable use of eval. Discuss with Engineering if this can be done more safely.

\sshell_exec\s*\(

ID: 175

warn

/home/chris/src/DVWA-master/vulnerabilities/exec/source/high.php:26

```
21:     $target = str_replace( array_keys( $substitutions ), $substitutions, $target );
22:
23:     // Determine OS and execute the ping command.
24:     if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
25:             // Windows
26:             $cmd = shell_exec( 'ping  ' . $target );
27:     }
28:     else {
29:             // *nix
30:             $cmd = shell_exec( 'ping  -c 4 ' . $target );
31:     }
```

It looks like it may be possible to perform a shell-injection here. Discuss with Engineering whether $target could be manipulated maliciously.

\supdate

ID: 101

critical

/home/chris/src/DVWA-master/vulnerabilities/captcha/source/high.php:**30**

```
25:             // CAPTCHA was correct. Do both new passwords match?
26:             if( $pass_new == $pass_conf ) {
27:                     $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_esc
28:                     $pass_new = md5( $pass_new );
29:
30:                     // Update database
31:                     $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "' LIMIT 1;";
32:                     $result = mysqli_query($GLOBALS["___mysqli_ston"],  $insert ) or die( '<pre>' . ((is_object($GLOBALS["___my
33:
34:                     // Feedback for user
35:                     $html .= "<pre>Password Changed.</pre>";
```

It looks very likely that the query executed on L32 is vulnerable to SQL injection. Discuss with Engineering immediately.