Mason Competitive Cyber

Meeting 6: More Web

Upcoming Events

- Bitcamp
  - This weekend @ UMD
  - Hackathon
- HackPSU
  - This weekend @ UMD
  - Bitcamp is better

News March31st-April7th

- N Korea Possibly Behind Bangladesh Bank Heist
  - 81 million (USD) stolen Bangladesh’s central bank
  - Biggest bank robbery ever → glorious leader does it again!
  - European Server used in heist has logs showing it connected to N Korea

- Breaches Don’t Fall Under General Liability Policy
  - St. Paul Fire & Marine Insurance has filed a lawsuit against Rosen Millennium Technology Group
  - Rosen breached, CC data stolen, fined by CC companies
  - Filed for reimbursement under Gen Liability

News March31st-April7th

- FBI and DHS disagree on when to notify victims that they’ve been breached
  - FBI wants information and admissible evidence
  - DHS wants to immediately stop and fix the breach

- Massive Brazilian Bank Hack
  - Kaspersky people revealed how it worked On Tuesday
  - Hack occurred in October 2016
  - Compromised bank’s account at a domain registration service
  - DNS Hijacking, which even shut down bank’s email
  - Phishing + Malware

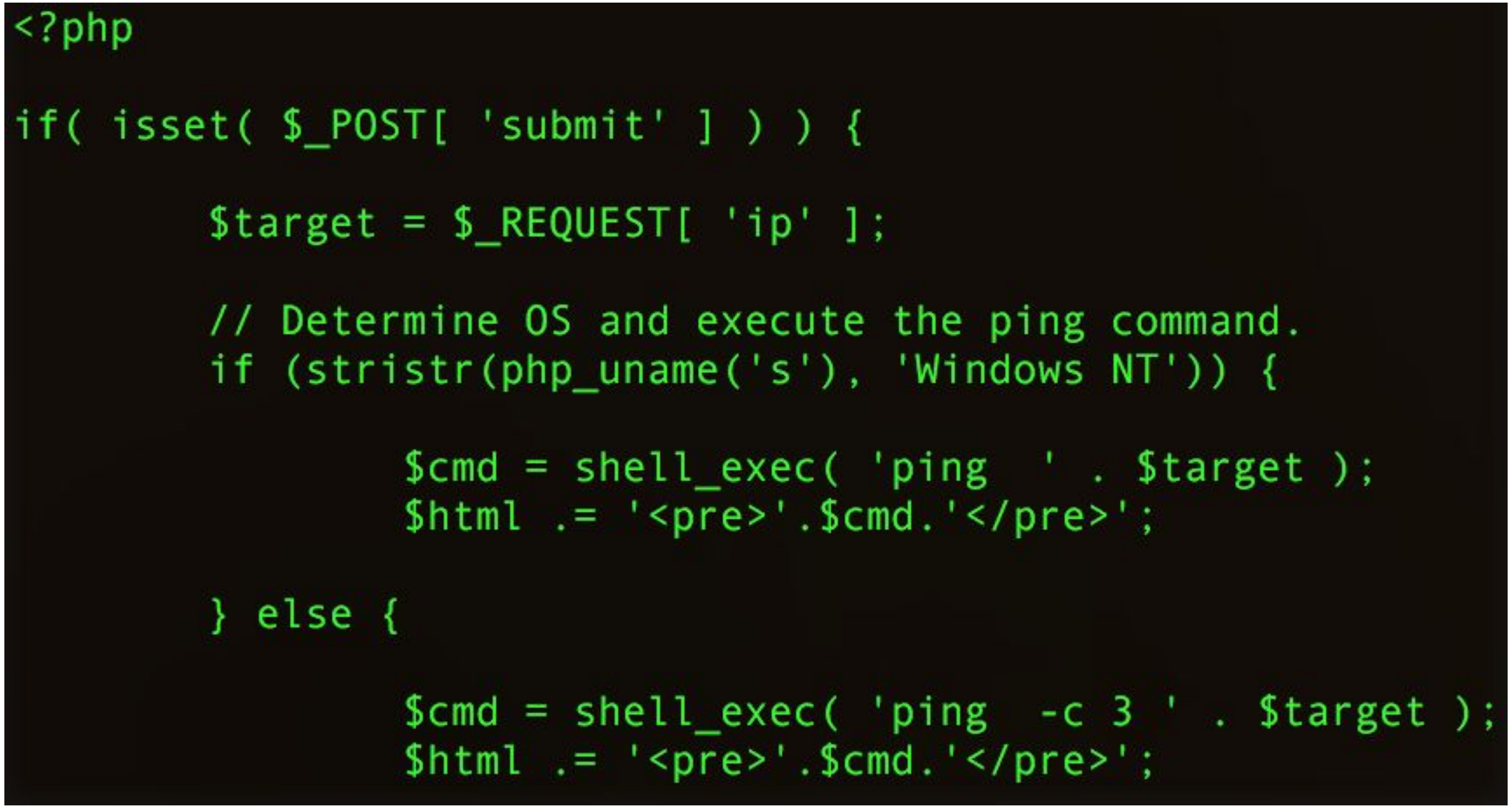
Damn Vulnerable Web App

- go.gmu.edu/damn

- admin
- password

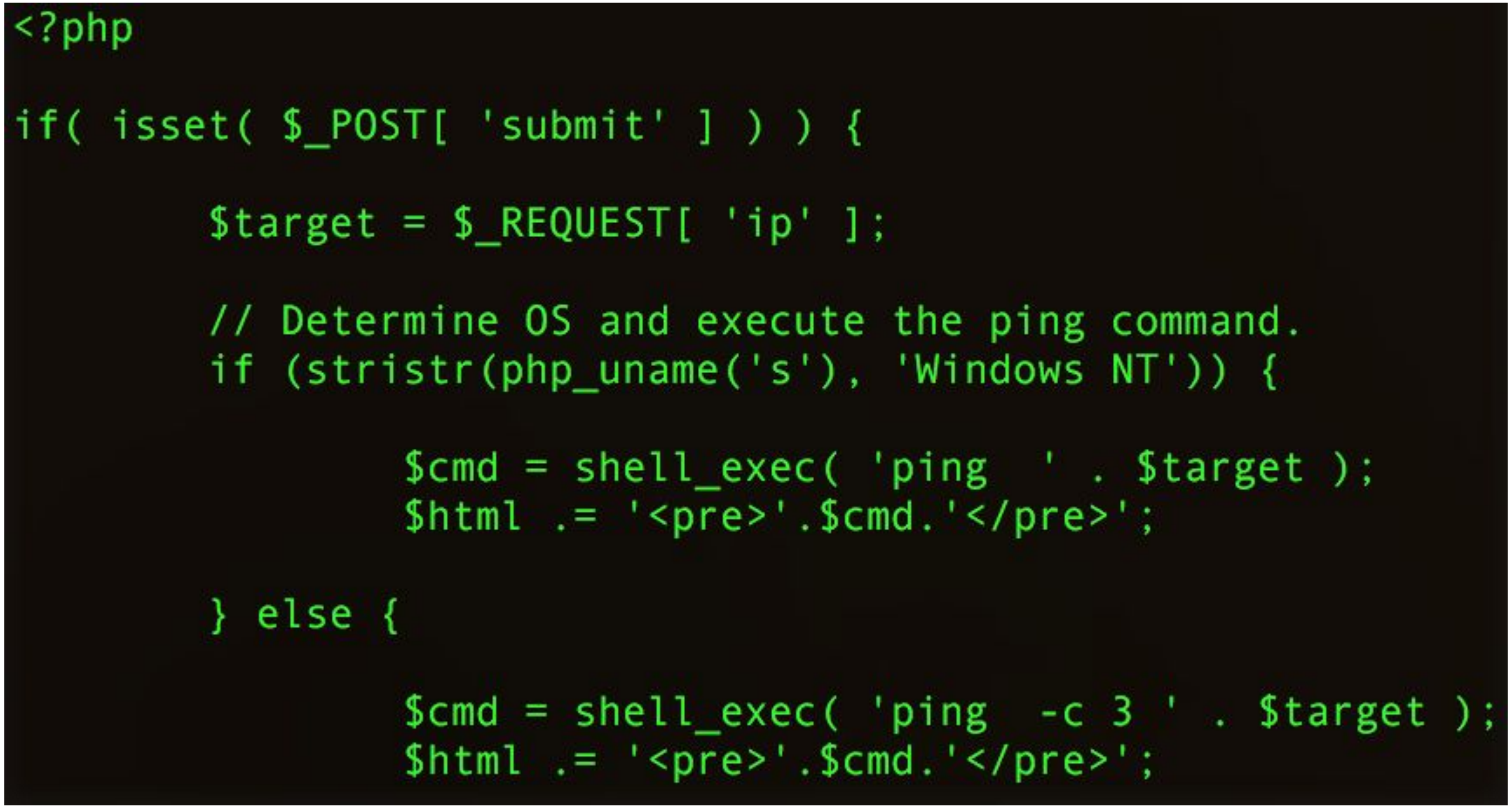
- 3 levels of difficulty
  - low - simple attacks
  - medium - slightly harder attacks
  - high - proper implementation, not supposed to be exploitable

What type of vulnerability is this?



```
<?php

if( isset( $_POST[ 'submit' ] ) ) {

        $target = $_REQUEST[ 'ip' ];

        // Determine OS and execute the ping command.
        if (stristr(php_uname('s'), 'Windows NT')) {

                $cmd = shell_exec( 'ping  ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';

        } else {

                $cmd = shell_exec( 'ping  -c 3 ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';
```

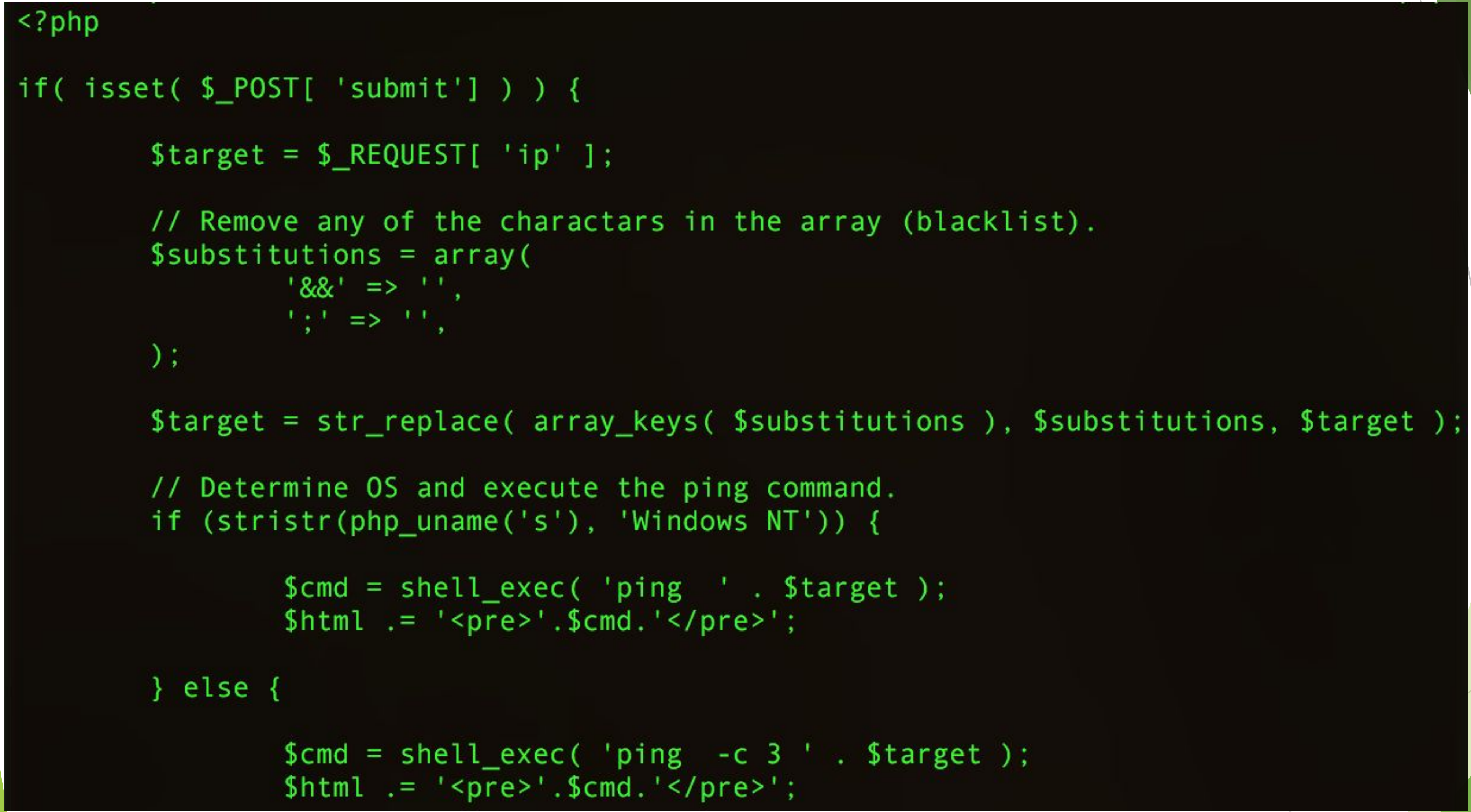
Command Injection (Low Difficulty)



```
<?php

if( isset( $_POST[ 'submit' ] ) ) {

        $target = $_REQUEST[ 'ip' ];

        // Determine OS and execute the ping command.
        if (stristr(php_uname('s'), 'Windows NT')) {

                $cmd = shell_exec( 'ping  ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';

        } else {

                $cmd = shell_exec( 'ping  -c 3 ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';
```

- $target could be any input

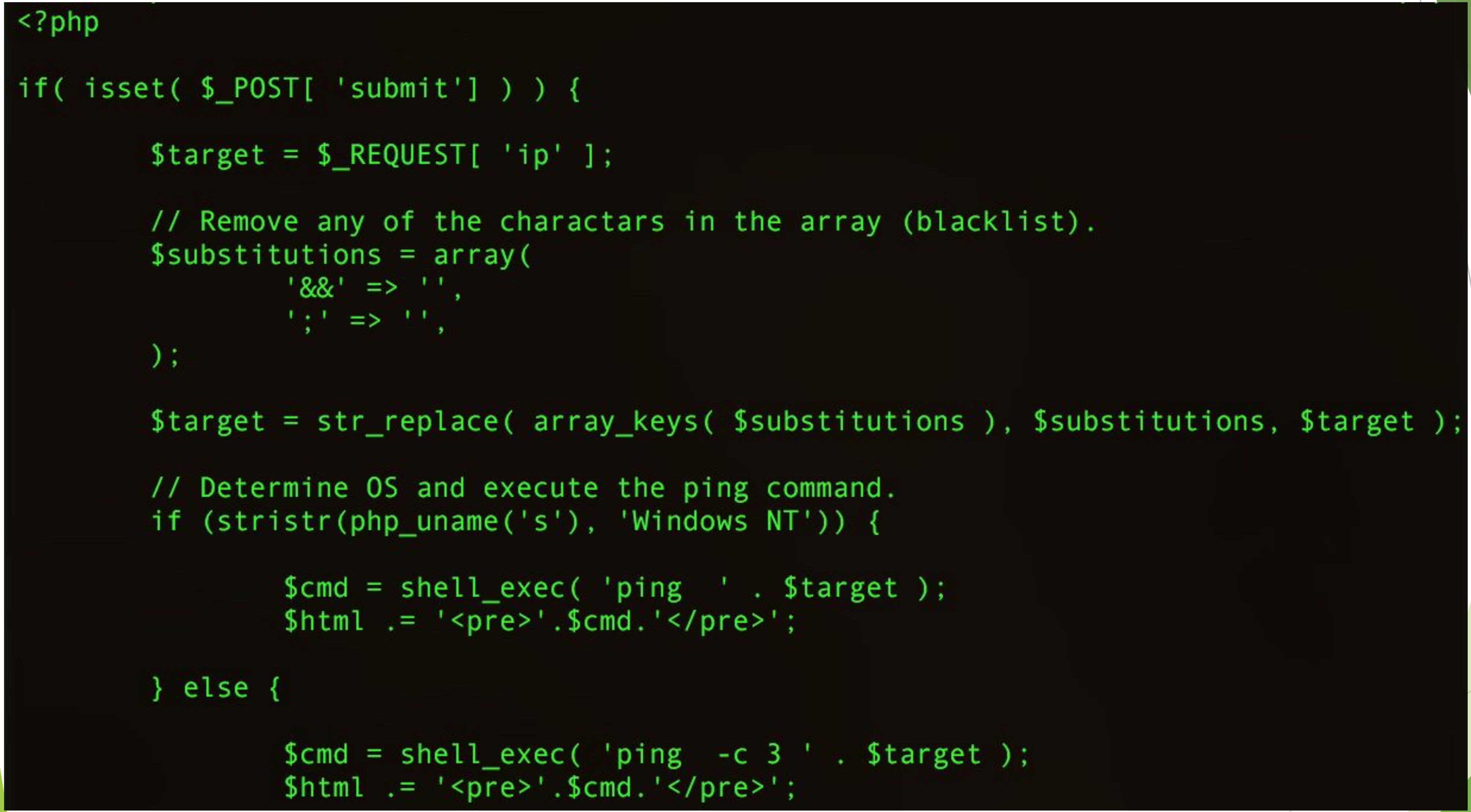
Command Injection (Medium Difficulty)



```
<?php

if( isset( $_POST[ 'submit'] ) ) {

        $target = $_REQUEST[ 'ip' ];

        // Remove any of the charactars in the array (blacklist).
        $substitutions = array(
                '&&' => '',
                ';' => '',
        );

        $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

        // Determine OS and execute the ping command.
        if (stristr(php_uname('s'), 'Windows NT')) {

                $cmd = shell_exec( 'ping  ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';

        } else {

                $cmd = shell_exec( 'ping  -c 3 ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';
```

- Can’t use && or ;

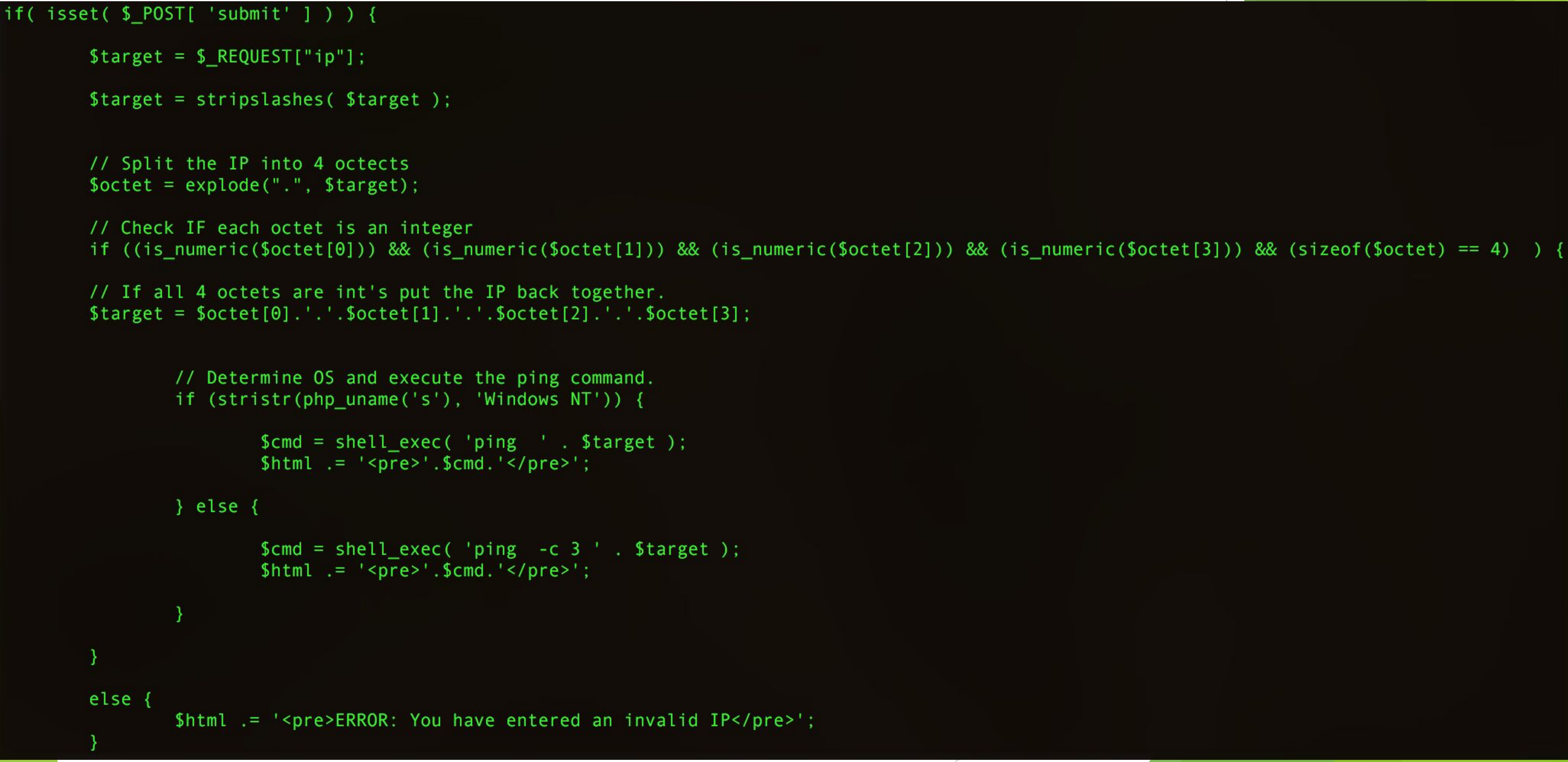
Command Injection (Medium Difficulty)



```
<?php

if( isset( $_POST[ 'submit'] ) ) {

        $target = $_REQUEST[ 'ip' ];

        // Remove any of the charactars in the array (blacklist).
        $substitutions = array(
                '&&' => '',
                ';' => '',
        );

        $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

        // Determine OS and execute the ping command.
        if (stristr(php_uname('s'), 'Windows NT')) {

                $cmd = shell_exec( 'ping  ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';

        } else {

                $cmd = shell_exec( 'ping  -c 3 ' . $target );
                $html .= '<pre>'.$cmd.'</pre>';
```

- Can use |

Command Injection (High Difficulty)



```
if( isset( $_POST[ 'submit' ] ) ) {

        $target = $_REQUEST["ip"];

        $target = stripslashes( $target );


        // Split the IP into 4 octects
        $octet = explode(".", $target);

        // Check IF each octet is an integer
        if ((is_numeric($octet[0])) && (is_numeric($octet[1])) && (is_numeric($octet[2])) && (is_numeric($octet[3])) && (sizeof($octet) == 4)  ) {

        // If all 4 octets are int's put the IP back together.
        $target = $octet[0].'.'.$octet[1].'.'.$octet[2].'.'.$octet[3];


                // Determine OS and execute the ping command.
                if (stristr(php_uname('s'), 'Windows NT')) {

                        $cmd = shell_exec( 'ping  ' . $target );
                        $html .= '<pre>'.$cmd.'</pre>';

                } else {

                        $cmd = shell_exec( 'ping  -c 3 ' . $target );
                        $html .= '<pre>'.$cmd.'</pre>';

                }

        }

        else {
                $html .= '<pre>ERROR: You have entered an invalid IP</pre>';
        }
```

Things to Remember

- OWASP Top 10 Web Vulnerabilities
- go.gmu.edu/owasp