

Class 07: Building a CMS with PHP and MySQL, and Website Security

Template-driven websites

How can PHP pass values from one page to another?

URL parameters

Multiple parameters

\$GET

Data validation

Sanitizing data

How websites are attacked

SQL injection

Hacking is easy

What hackers can do

Precautions (how to protect yourself)

What to do if you are hacked

References

PHP and MySQL for Dynamic Web Sites 5th Ed. by Larry Ullman

Head First PHP & MySQL by Lynn Beighley and Michael Morrison

PHP Solutions: Dynamic Web Design Made Easy 2nd Ed. by David Powers

Homework

Read: Chapter 10 of PHP and MySQL for Dynamic Web Sites

OR Chapter 5 of Head First PHP & MySQL

<http://www.creativebloq.com/web-design/website-security-tips-protect-your-site-7122853>

The “takeaway” from this week’s session is that you should be aware of website security issues, take precautions to avoid problems and always filter and/or sanitize any data that originates from outside a PHP script before using it. A simple test will do the job:

```
if (isset($_GET['id']) && filter_var($_GET['id'], FILTER_VALIDATE_INT)) {  
    $article=$_GET['id'];  
}else{  
    header('HTTP/1.0 404 Not Found');  
    exit("<h1>Not Found</h1>\n<p>The submitted data is not valid.</p>");  
}
```

The code above tests to see if a value exists and if that value is an integer.

Take a look at the Articles website and make sure you understand how it works.

Prepare for the Major Project firmness crit.

Course materials: [Content Management](#)