THE WORDPRESS SECURITY FEATURES WE DON'T SEE

FRANCESCO CARLUCCI AKA FRENXI
MY NAME IS FRANCESCO

FULL STACK DEVELOPER
WP EXPERT AT CODEABLE
SECURITY RESEARCHER BY NIGHT
THE ETERNAL QUESTION: IS WP SECURE?
WHY WE’RE STILL DISCUSSING IT?
BECAUSE IT DEPENDS...
LET'S TRY A NEW APPROACH
HOW WOULD YOU JUDGE A BAD PERSON?
I DON'T KNOW!

BUT FOR SURE, A BAD PERSON DOES BAD THINGS!
WHAT IF WE TRY TO JUDGE SOFTWARE THE SAME WAY WE WOULD JUDGE PEOPLE?
WE HAVE A BENEFIT!

IN SOFTWARE DEVELOPMENT
BAD THINGS ARE CLEARLY BAD
NO ROOM FOR DISCUSSION
THE IMPORTANCE OF COOKIES
HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:69.0)
Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en,en-US;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: [long string]
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
A COOKIE IS AS IMPORTANT AS YOUR PASSWORD
WHAT CAN POSSIBLY GO WRONG?
setcookie

(PHP 4, PHP 5, PHP 7)

setcookie — Send a cookie

Description

setcookie ( string $name [, string $value = "" [, int $expires = 0 [, string $path = "" [, string $domain = "" [, string $secure = FALSE [, bool $httponly = FALSE ]]]]]]) : bool

setcookie ( string $name [, string $value = "" [, array $options = [] ]]) : bool

setcookie() defines a cookie to be sent along with the rest of the HTTP headers. Like other headers, cookies must be set from your script (this is a protocol restriction). This requires that you place calls to this function prior to any output, in <head> tags as well as any whitespace.

Code Reference

Browse: Home / Reference / Functions / wp_set_auth_cookie()

wp_set_auth_cookie( int $user_id, bool $remember = false, mixed $secure
string $token = "")

Log in a user by setting authentication cookies.
OK... ENOUGH COOKIES FOR TODAY...
CSRF Attack

- Assume that the victim is logged-in to www.bofw.com

```html
<form action="https://bofw.com/xfer.php">
  <input type="hidden" name="to" value="attacker">
  <input type="hidden" name="amount" value="1000000">
</form>
<script>document.forms[0].submit();</script>
```
CSRF IS VERY COMMON ALSO ON LARGE AND WELL KNOWN WEBSITES!

WORDPRESS HAS NONCES TO PREVENT IT!
AND THEN, THE (PROBABLY) MOST COMMON VULNERABILITY IN WEB APPLICATIONS
XSS
CROSS SITE SCRIPTING
HOW DOES IT WORK
WHY IS SO COMMON
WHY IS SO DANGEROUS
ECHO $_GET["PARAM"];
How to Discover 1352 Wordpress Plugin XSS 0days in one hour

(Not Really)

v1.9
Larry W. Cashdollar
Jeffcon Jr.
Specials Workshop
WHAT??

98% WERE FALSE POSITIVE!
BECAUSE WORDPRESS ESCAPES SUPER GLOBAL VARIABLES
/**
 * Add magic quotes to `$_GET`, `$_POST`, `$_COOKIE`, and `$_SERVER`.
 *
 * Also forces `$_REQUEST` to be `$_GET + $_POST`. If `$_SERVER`,
 * `$_COOKIE`, or `$_ENV` are needed, use those superglobals directly.
 *
 * @since 3.0.0
 * @access private
 */

function wp_magic_quotes() {
    // If already slashed, strip.
    if ( get_magic_quotes_gpc() ) {
        $_GET    = stripslashes_deep( $_GET );
        $_POST   = stripslashes_deep( $_POST );
        $_COOKIE = stripslashes_deep( $_COOKIE );
    }

    // Escape with wpdb.
    $_GET    = add_magic_quotes( $_GET );
    $_POST   = add_magic_quotes( $_POST );
    $_COOKIE = add_magic_quotes( $_COOKIE );
    $_SERVER = add_magic_quotes( $_SERVER );

    // Force REQUEST to be GET + POST.
    $_REQUEST = array_merge( $_GET, $_POST );
}
“SECURITY IS A PROCESS, NOT A PRODUCT”
(BRUCE SCHNEIER)

THANK YOU!