# Cross Site Request Forgery

CYBER SECURITY & PRIVACY FOUNDATION

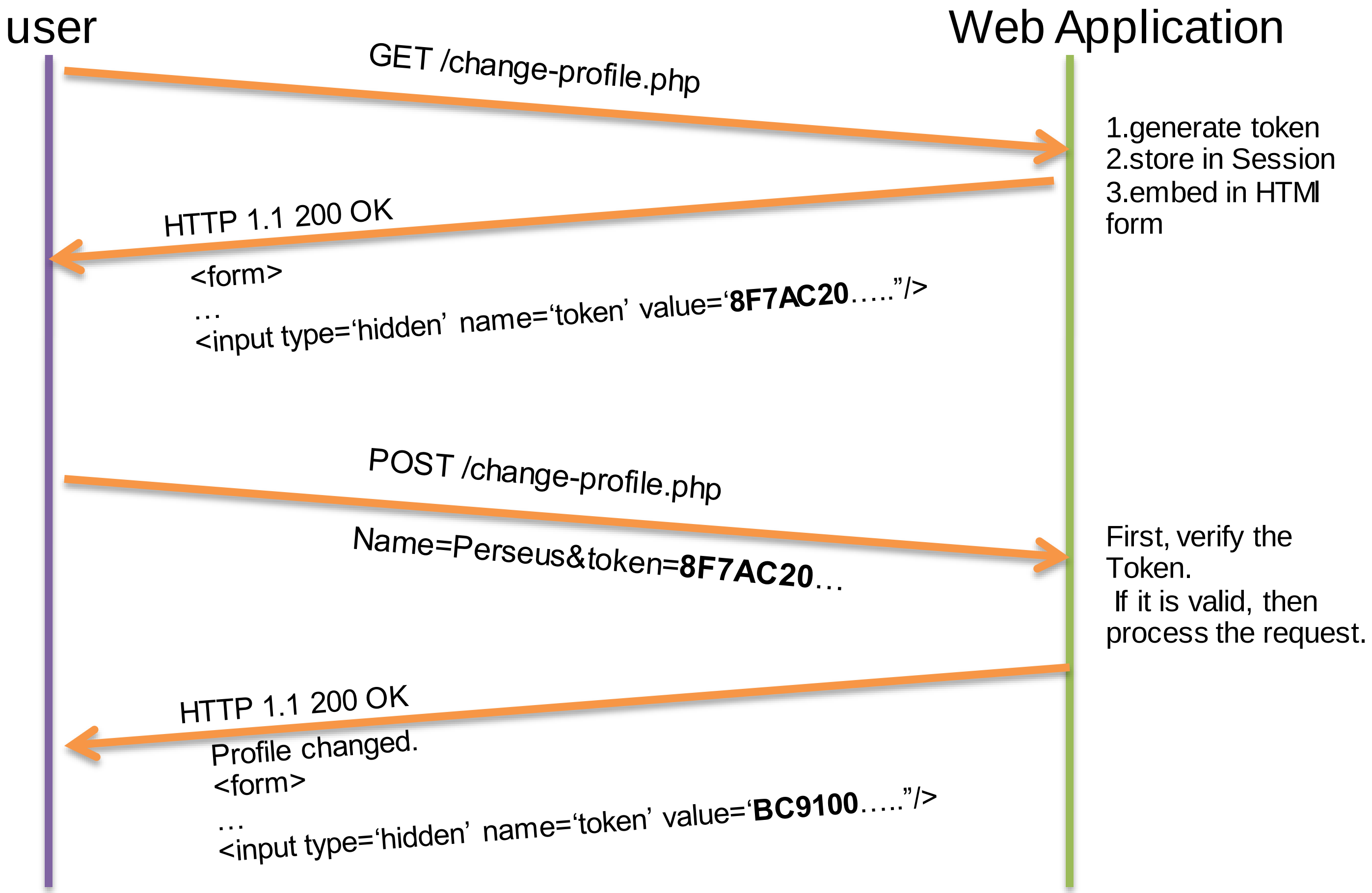
Synchronizer Token Pattern

Challenge Response

NO XSS

# Synchronizer Token Pattern

- The best CSRF prevention measure
- A challenge token is embedded by the web application in all HTML forms and verified on the Server side.
- The token should be a unique cryptographic value for every HTTP requests and should be random.
- The Token value will be stored in the User’ session so that server can verify it.



user

Web Application

GET /change-profile.php

1.generate token
2.store in Session
3.embed in HTMl
form

HTTP 1.1 200 OK

```
<form>
…
<input type=‘hidden’ name=‘token’ value=‘8F7AC20…..”/>
```

POST /change-profile.php

Name=Perseus&token=**8F7AC20**…

First, verify the
Token.
 If it is valid, then
process the request.

HTTP 1.1 200 OK

```
Profile changed.
<form>
…
<input type=‘hidden’ name=‘token’ value=‘BC9100…..”/>
```

# Example PHP Code for generating Token

```
<?php
    $token = sha1(uniqid(mt_rand(0,100000)));
    $_SESSION["token"] = $token;
?>
```

# Example PHP Code for Embedding the Token in HTML form

```
<form action=‘request.php’ method=‘POST’>

<input type=‘text….

….

<input type=‘hidden’ name=‘token’ value=“<?php echo
    $_SESSION[‘token’]; ?>”/>

</form>
```

# Example PHP Code for verifying the CSRF Token

```
<?php
….
if(isset($_POST[‘token’]) && $_SESSION[‘token’]==$_POST[‘token’])
{
//Process the request
..
}
else
{
echo “CSRF token is missing”;
}
```

# Challenge Response

- ➢ In Sensitive functions such as money transfers or password change, it is better to add additional authentication.
- ➢ The following are some examples of challenge-response options.
  - ✓Two factor Authentication
  - ✓Re-Authentication (Password)
  - ✓CAPTCHA

# No XSS

- Cross site Scripting(XSS) vulnerabilities allows attacker to bypass the CSRF Defenses.
- A XSS payload can read the HTML page and obtain the CSRF token.
- It is imperative that no XSS vulnerabilities are present to ensure that CSRF defenses can't be circumvented.