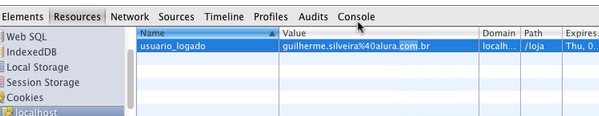
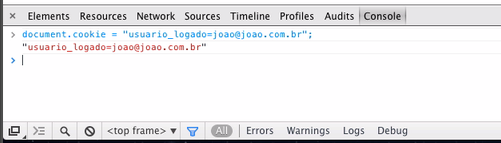
**Insegurança com cookie, segurança com session e efetuando logout**

Criamos uma loja, adicionamos o sistema de login e protegemos nossa página. Mas nosso cliente, administrador da loja, nos liga dizendo que tem uma pessoa qualquer logado com o usuário dele. Como assim? Não nos protegemos?

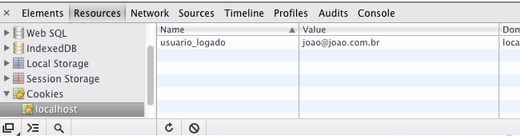
Vamos dar uma olhada no que acontece com os cookies? Nos logamos no sistema e verificamos o cookie:



Lembra que o cookie fica no cliente? Como não temos controle sobre o cookie, será que o cliente consegue alterar ele? Com certeza, ele pode fazer o que quiser com os cookies, não temos como saber. Executamos, por exemplo, um código na aba de console para alterar o valor de um cookie:



Voltamos na aba de resources e nosso cookie se tornou:



Agora podemos voltar a home e temos que o usuário logado é o:



Podemos usar cookies mas não adicionar valores claramente de segurança em dados do cliente. Não podemos colocar seu email, seu id ou qualquer outra coisa similar. Devemos adicionar um código difícil de "chutar", um código qualquer para cada usuário como "74923878r8y9fwe8hr32nu" para esse usuário específico e "79y2huifenbu9fv98" para o próximo.

Gerando códigos muito diferentes para cada usuário faz com que eles não possam ficar chutando sem serem percebidos (muitas requisições). Para isso é importante usar um gerador bem elaborado. E do lado do servidor temos que atrelar a informação "74923878r8y9fwe8hr32nu" com "usuario\_logado = guilherme.silveira@alura.com.br". Assim o cliente só consegue alterar o valor do cookie, mas não existe nada no servidor para um número de cookie que não existe! Perfeito. Esse é o conceito de sessão: damos um código gerado para o cliente e do lado do servidor armazenamos este código com uma série de chaves e valores. O cliente só pode alterar aquele código, e terá que chutar muito para encontrar outro código válido.

Como mudamos para deixar de usar cookie e passar a usar sessão? Bom tudo será feito com o usuário logado, isto é, no único arquivo que usa os cookies, o **logica-usuario**. Primeiro, no começo do arquivo, devemos indicar que usaremos a sessão. Se não existe uma sessão ainda, desejamos criá-la, e se ela já existe, desejamos usá-la:

<?php

session\_start();

function usuarioEstaLogado() {

# codigo da função

}

# resto do arquivo aqui

Como colocar o usuário logado? O **logaUsuario**? Simples:

function logaUsuario($email) {

$\_SESSION["usuario\_logado"] = $email;

}

Para verificar se o usuário está logado basta chamarmos o método de usuario logado:

function verificaUsuario() {

if(!usuarioEstaLogado()) {

header("Location: index.php?falhaDeSeguranca=true");

die();

}

}

E como verificar se ele está logado? Basta verificar se **isset** esta variável:

function usuarioEstaLogado() {

return isset($\_SESSION["usuario\_logado"]);

}

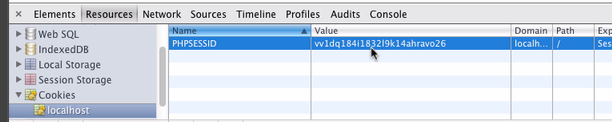
Por fim, o método que extrai o usuário logado:

function usuarioLogado($email) {

return $\_SESSION["usuario\_logado"];

}

Repare como foi fácil trocar todas as invocações de cookie para sessão! Acessamos agora nosso navegador e temos o novo cookie, o cookie que o PHP utiliza para marcar a sessão:



Ao nos logarmos, não há nada de diferente nos cookies. O valor do usuário logado fica armazenado no servidor e não no cliente! Agora como fazemos o logout?

Primeiro queremos um link de logout na página inicial, caso você esteja logado:

<?php if(usuarioEstaLogado()) {?>

<p class="text-success">Você está logado como <?= usuarioLogado() ?>.

<a href="logout.php">Deslogar</a></p>

<?php } else {?>

Precisamos criar o **logout.php**. Mais simples do que o login, ele chama uma função de logout e redireciona:

<?php include("logica-usuario.php");

logout();

header("Location: index.php?logout=true");

die();

Vamos agora criar a função logout no logica-usuario destruindo nossa sessão:

function logout() {

session\_destroy();

}

E no **index.php** vamos mostrar a mensagem de deslogado:

<?php

if(isset($\_GET["logout"]) && $\_GET["logout"]==true) {

?>

<p class="alert-danger">Deslogado com sucesso</p>

<?php

}

Vamos no navegador, clicamos deslogar e.. perfeito, deslogado com sucesso.