08

Forçando senhas com o GoogleRecaptcha

Transcrição

Neste vídeo, o IP de acesso ao Localhost do Windows na máquina do instrutor mudou de `http://192.168.121.171:8080/alura-shows/` para `http://192.168.121.100:8080/alura-shows/`. Lembrando que em seu computador, o IP do Localhost será diferente, para verificar digite `ipconfig` no Prompt de Comando.

Voltaremos para o Kali Linux para verificar qual será o resultado que o Alex irá obter no ataque de força bruta. Antes da implementação do *reCAPTCHA*, ele usou o ***Burp Suite*** para inserir de forma automatizada diversas senhas, o que resultou na descoberta da senha `789` cadastrada pela Ana. Essa descoberta aconteceu por ser a única senha a ter o status **HTTP 200**.

Novamente abriremos o *Burp Suite*. No pop-up ***Burp Suite Free Edition*** clicaremos em "OK", em seguida clicaremos em "Next" e depois em "Start Burp" para inicializar o programa. O primeiro passo é indicar para o *Burp Suite* quais são as URLs que queremos interceptar, no caso nó queremos todas relacionadas a aplicação da **Alura Shows**.

Vamos em "Target > Scope > Target Scope" e clicaremos em ***Add***. Em ***Host or IP range*** colocaremos o endereço da aplicação `http://192.168.121.100:8080/alura-shows/` e clicaremos em "OK".

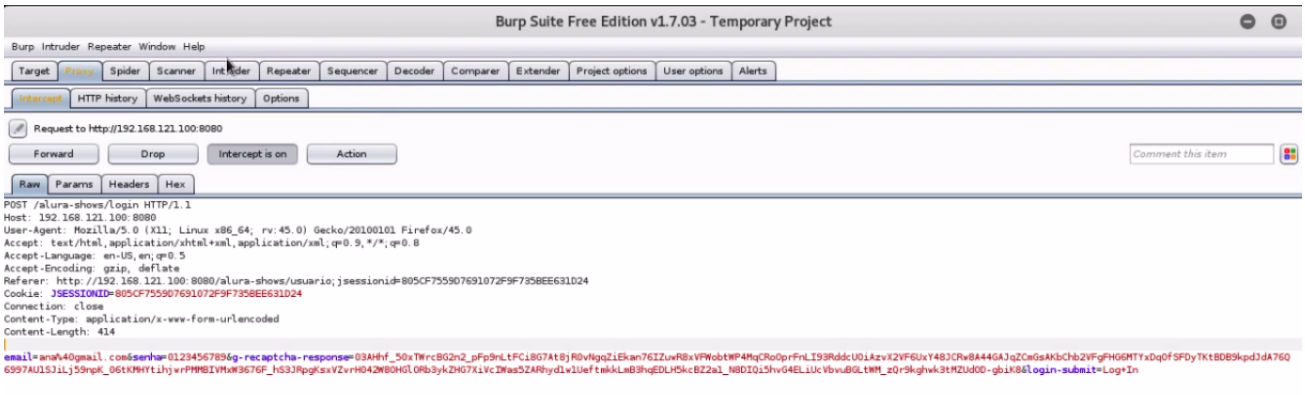
Quando adicionamos uma URL, o *Burp Suite* já começa a interceptá-la automaticamente. Por isso vamos em "Proxy > Intercept" e clicaremos em ***intercept is on*** para desativá-lo, pois ainda precisamos de mais algumas configurações. Ao desativar, o botão ficará como ***intercept is off***.

Acessando "Proxy > Options > Proxy Listeners" veremos que o *Burp Suite* está escutando na porta `127.0.0.1:8080`. Dessa forma, é necessário configurar o navegador Firefox para enviar as requisições para o endereço que o *Burp Suite* está escutando. No Firefox do Linux, vamos em "Menu > Preferences > Advanced > Configure", selecionaremos a opção ***Manual proxy configuration***, na seção ***HTTP Proxy*** colocaremos `127.0.0.1`, na seção ***Port*** colocaremos `8080`.

No *Burp Suite* acessaremos "Proxy > Intercept", e clicaremos no botão ***Intercept is off***, ele ficará como ***intercept is on***.

No Firefox acessaremos a tela de *login* da aplicação, para o campo **E-mail** colocaremos `ana@gmail.com`, no campo **Senha** colocaremos `0123456789`, essa é uma senha que o Alex acredita ser utilizada pela Ana. Clicaremos no botão do *reCAPTCHA* e em "LOG IN".

De volta no *Burp Suite*, acessaremos "Proxy > Intercept > Raw". Vemos que a requisição foi interceptada:



Clicando com o botão direito do mouse, selecionaremos a opção ***Send to Intruder***. Em "Intruder > 2 x > Positions" veremos diversos campos selecionados, clicaremos em "Clear" para limpar todos os campos e selecionaremos apenas o valor da senha e clicaremos em "Add".

Agora em "Intruder > 2 x > Payloads > Payloads Options [Simple list]", colocaremos a opção de senha no campo ***Enter a new item*** e adicionaremos a lista clicando em "Add". A lista de senha será:

- alura
- ana_alura
- 012345
- 0123
- 789
- alura_ana
- admin
- ana_admin
- ana_alura_shows
- 987654321

Colocamos algumas senhas e dentre elas, temos a senha correta `789` utilizada no cadastro da Ana. Antes da implementação do *reCAPTCHA*, o teste de força bruta retornou o status **HTTP 200** para a senha `789`, indicando que ela era a senha correta.

Executaremos o teste clicando em ***Start attack***. Repare que agora todas as senhas, incluindo a `789`, retornaram o status **HTTP 302**, isso aconteceu porque o *reCAPTCHA* não foi validado pelo Google. O status **302** é de redirecionamento, o *Burp Suite* tentou efetuar o *login* mas como o Google não validou o clique no *reCAPTCHA*, a aplicação redirecionou para o formulário novamente.

Dessa forma, o Alex não conseguirá saber qual senha foi usada pela Ana em seu cadastro.