**Kịch bản:** Tại phần nhập mật khẩu

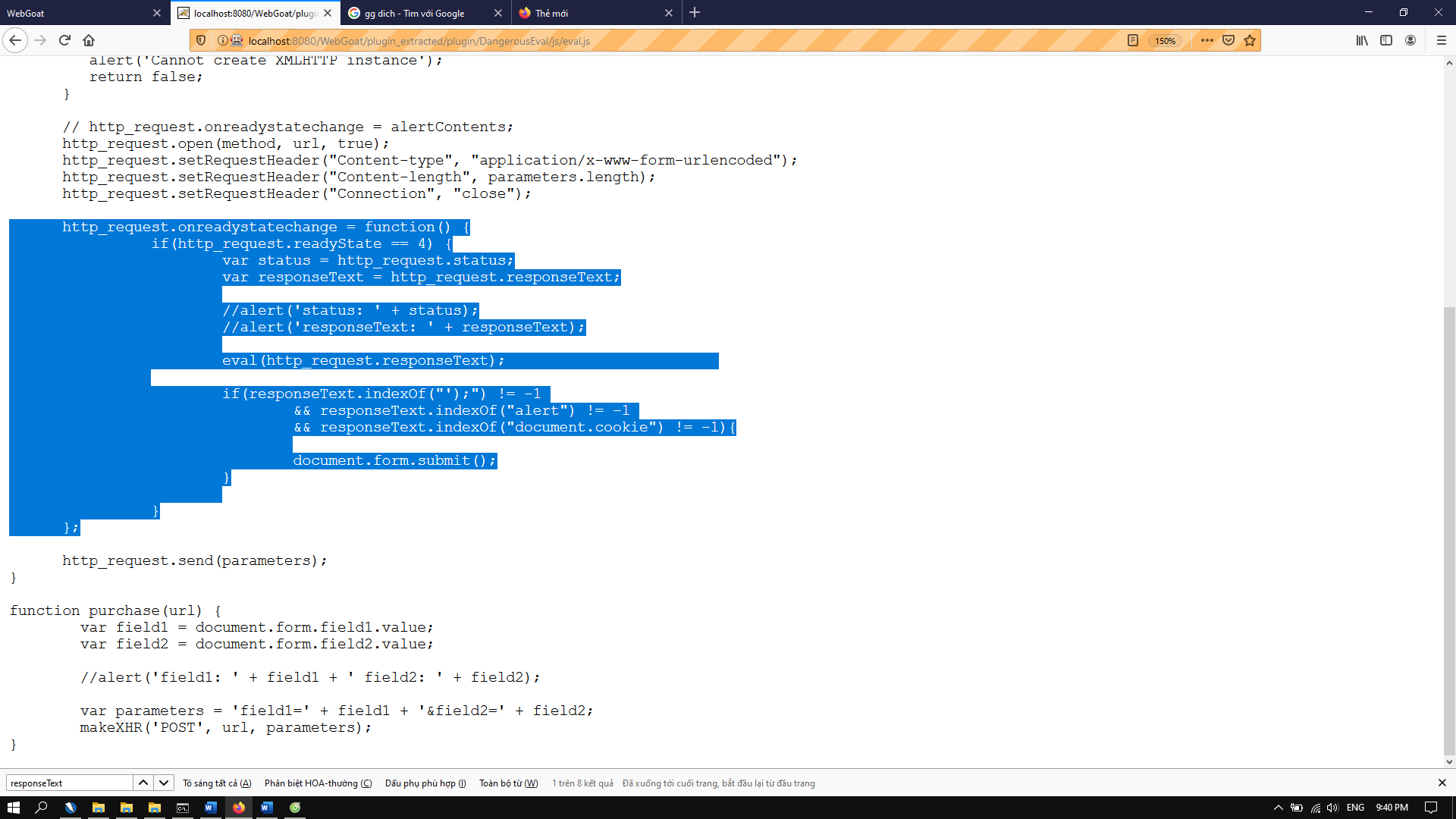
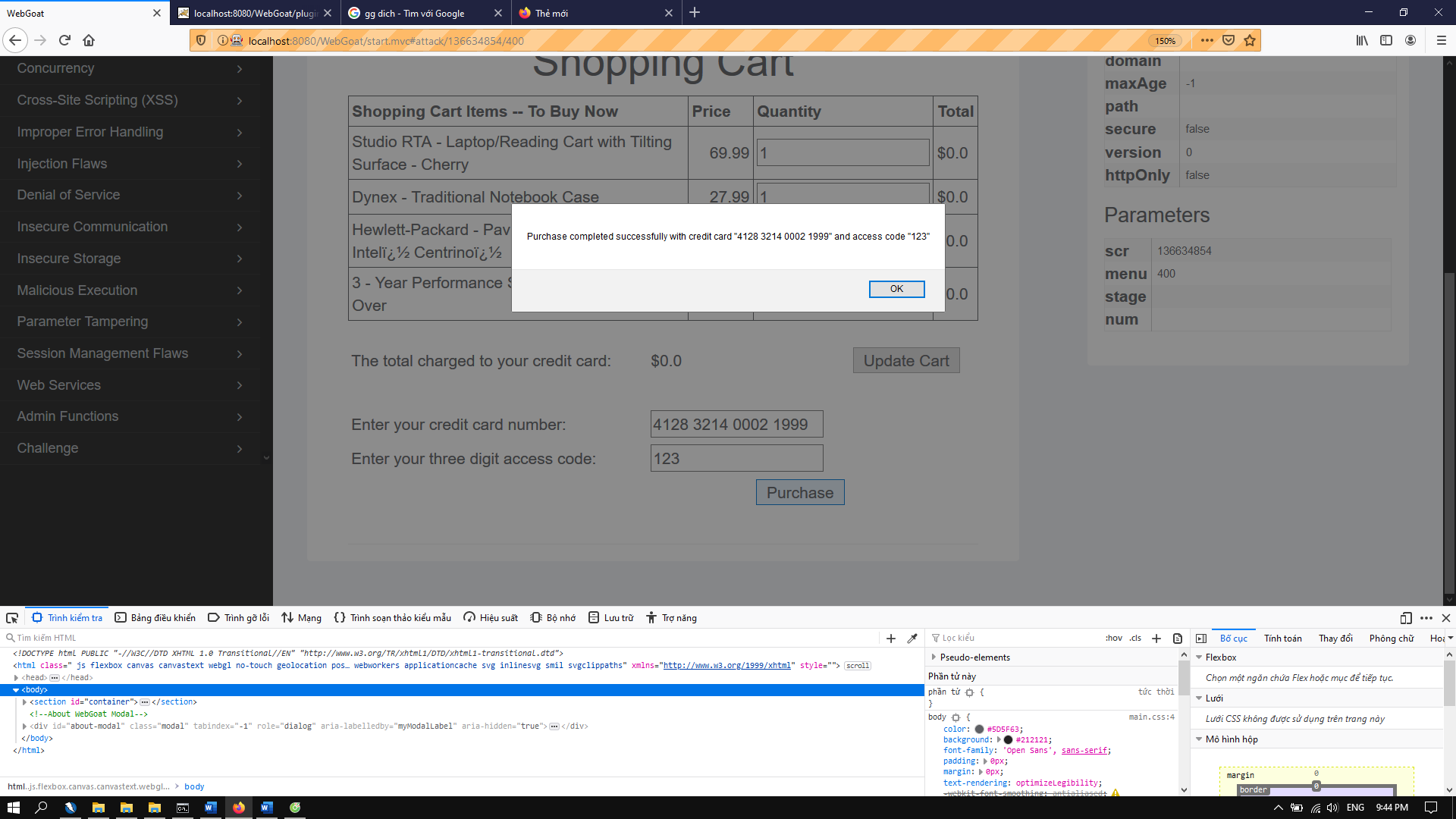
**Mục tiêu:** Lấy được Cookie

**Giải thích:** Khi render, var parameters = 'field1=' + field1 + '&field2=' + field2; sẽ được gán cho hàm makeXHR(). Để lấy được request ta cần thay đổi giá trị trong field1 để đánh lừa Server khi Response

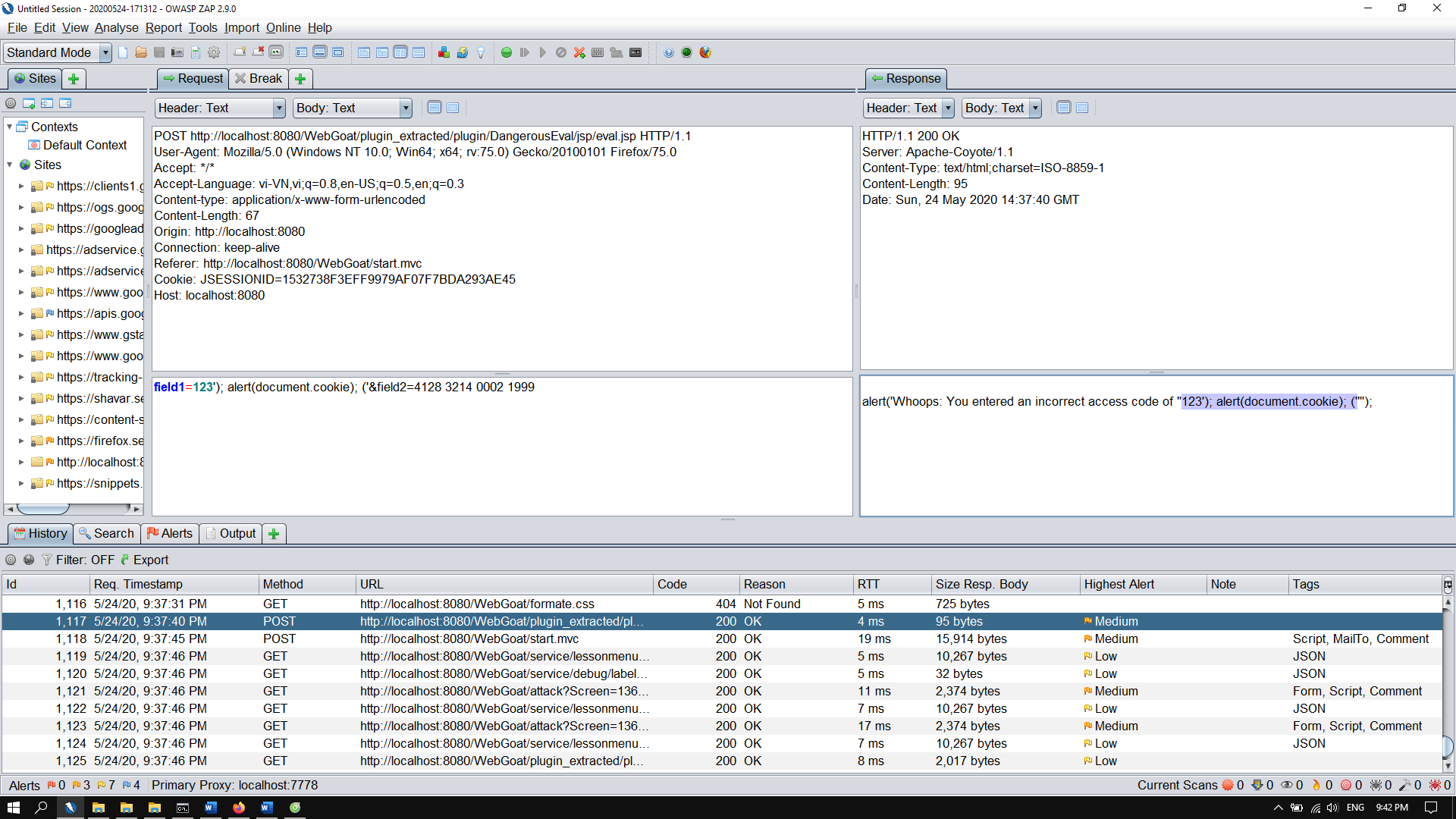
Giá trị server response vào Eval() sẽ là

Eval(Purchase completed successfully with credit card "**PARAMETER2**" and access code "**PARAMETER1**");

Vậy theo thuật toán thì http\_request.responseText = ’SomeMessage”P1”SomeMessage”P2”’



Qua đó ta có thể lợi dụng Event onreadystatechange với State = 4 này để thực thi một đoạn Script với Script sẽ được chèn tại Param1 tức TextBox Digital Code



Vậy kết quả sau khi tiến hành sẽ là: 123');alert(document.cookie);('

* eval('123');alert(document.cookie);(''); qua đó ta sẽ lấy được Cookie sau khi trả về của Web