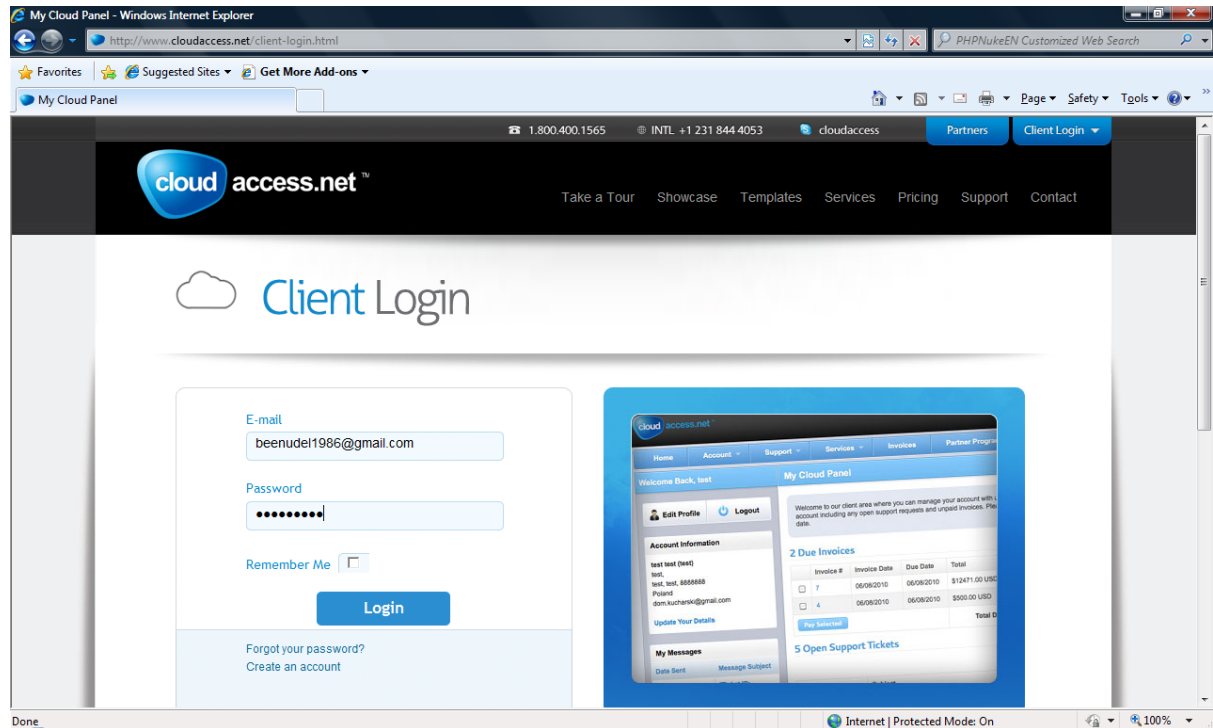


Joomla CSRF Vulnerability

Target Page: Edit Profile

POC:

Login to Joomla portal:



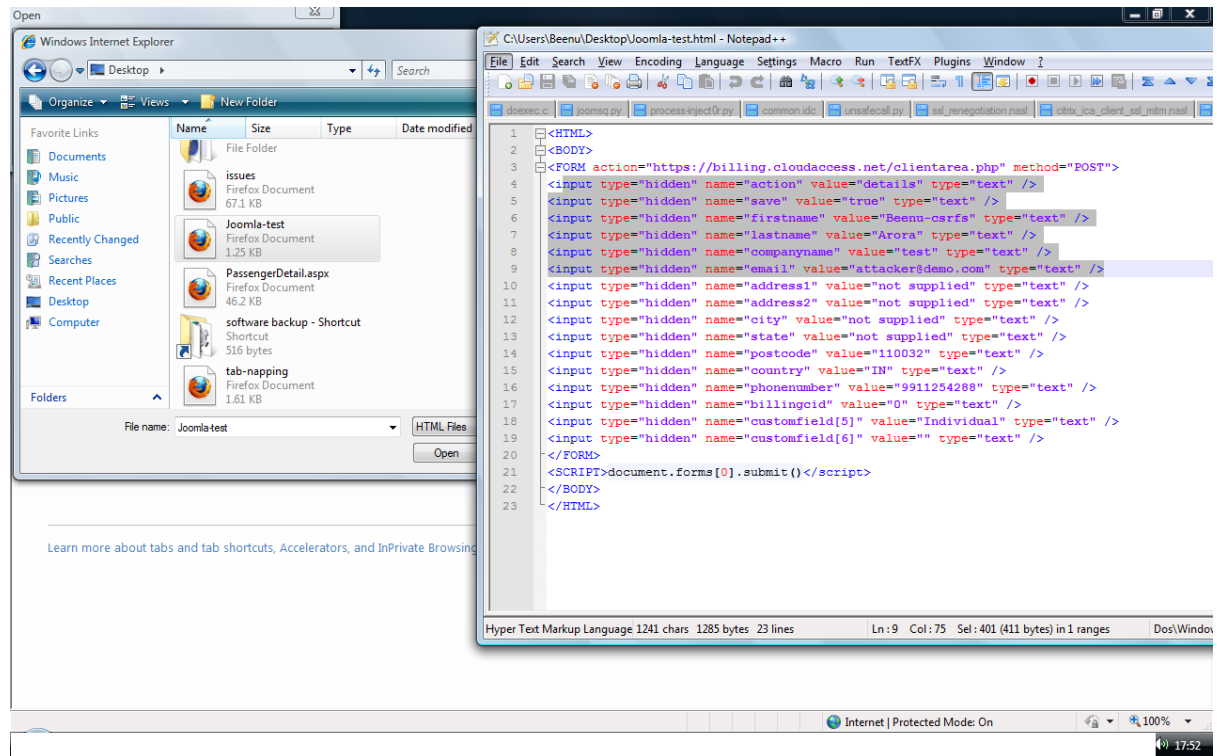
Edit profile page showing the profile information.

The screenshot displays the 'Edit Profile' page within the CloudAccess.net Client Area. The browser window title is 'CloudAccess.net - Client Area - Windows Internet Explorer'. The address bar shows 'https://beenu.cloudaccess.net/clientarea.php?action=details'. The page features a navigation bar with links: Home, Account, Support, Services, Invoices, Partner Program, My Messages, and Logout. Below this, a 'Welcome Back, Beenu' message is shown alongside 'Edit Profile' and 'Logout' buttons. The 'Account Information' section lists: Beenu Arora (test), not supplied, not supplied, not supplied, 110032, India, and beenudel1986@gmail.com, with an 'Update Your Details' link. The 'My Messages' section shows a message from 'Your Joomla! trial login' dated 09/22/2010 07:03, with a 'Show All...' link. The 'Edit Profile' form contains the following fields:

Field	Value
First Name	Beenu
Last Name	Arora
Company Name	test
Email Address	beenudel1986@gmail.com
Address 1	not supplied
Address 2	not supplied
City	not supplied
State/Region	not supplied
Zip Code	110032
Country	India

The browser status bar at the bottom indicates 'Internet | Protected Mode: On' and '100%' zoom.

Malicious page opened in the new tab to update first name and email id.



Page opened; as a result the profile gets updated.

