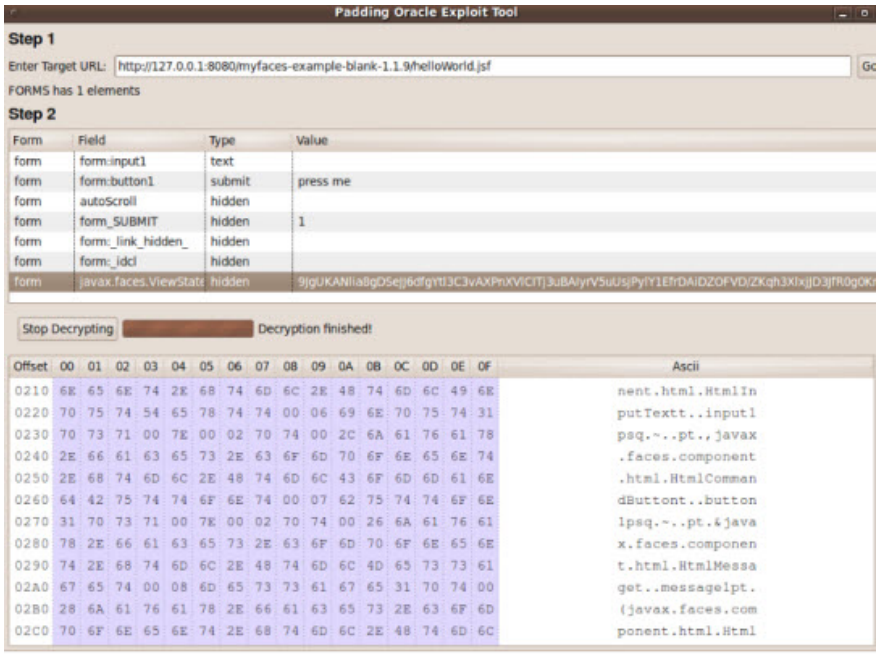
Tool to unlock data encryption sessions - CAPTCHAS

Recently, two researchers have released a tool that can be used to unlock encrypted data via the web server system contained in cookies and hidden characters in HTML pages.

***TipsMake.com* - Recently, two researchers have released a tool that can be used to unlock encrypted data via web server system contained in cookies and hidden characters in HTML pages** . This method is used in Juliano Rizzo and Thai Duong's Padding Oracle Exploitation Tool (Poet), and is also used to crack CAPTCHAS.

Poet used in Padding Oracle AttackPDF, first discovered in 2002, is used to decode Cypher Block Chaining (CBC) mode without key. The above web applications use the popular JavaServer Faces (JSF) framework, which is easily exploited in this way.



The Padding Oracle Attack attack mechanism has shown that the actual encryption blocks must have a minimum length of 8 or 16 bytes per character. But to meet the requirements, these mechanisms must use additional bytes for the final blocks. Besides, there are many ways to implement this supplementary mechanism, and one of them uses crack. This is the time that Padding Oracle - the necessary program or service is used to inform the status to indicate whether the addition of capacity in received packets is considered valid, and continue. Continue to participate in the overall process. This is exactly what the JFS framework demonstrates.

By trying all the other complementary and possible ways, this mechanism can completely decode ViewStates, which is embedded in the HTML page and used to store traffic information from the client quickly. You can watch the video demonstrating this process on Youtube.

[youtube] http://www.youtube.com/watch?v=euujmKDxmC4 [/ youtube]

The decrypted data also stores the amount of confidential information that website visitors do not have access to. This attack mechanism is described fully and thoroughly here.

On the other hand, this technology is also used to code other solutions, one of which is the existing image character encoding - typically CAPTCHAS. To avoid storing this information, some server systems transfer all data to the client and then compare it with the return signal.

Although Poet can only crack ViewStates, this is enough to help developers test and detect vulnerabilities on their websites. This tool has GUI interface and works with Windows, Mac OS X and Linux.