

Using Pastebin Sites for Pen Testing Reconnaissance

Text-sharing “pastebin” sites, such as [Pastebin](#) and [Pastie](#) are a popular repository of compromised data. Keeping an eye on these websites can help identify a breach related to your organization, [as I wrote earlier](#). They can also help during the reconnaissance phase of a penetration testing project, allowing the assessor to collect sensitive information about the target for follow-up attacks.

The sites to which I am referring are designed for sharing text over the web, such as: [Pastebin](#), [Pastie](#), [FrubarPaste](#), [Codepad](#) and [Slexy](#). In some cases, perpetrators of computer breaches post the data they have stolen on such sites. Sometimes, sensitive information is unwittingly leaked by a company’s employee.

An Internet-based penetration tester often begins the project by mining public data to identify sensitive details regarding the target. This reconnaissance stage of the assessment is typically used as the base for launching further attacks. When conducting such a project, consider

MORE ON

Consulting Research

Information Security

SHARE ➞

including the text-sharing sites mentioned above in your search, mining them for records related to the target, such as:

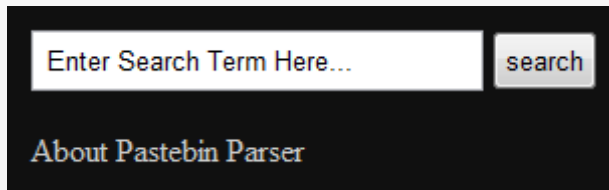
- Stolen data, such as credit card numbers or PII
- Source code snippets that might reveal website inner-workings
- Configuration details of network devices
- Employee names, contact details and job functions

To see the kind of data you can locate on text-sharing sites, take a look at Silas Cutler's post [The Dangers of Pastebin Sites](#). Silas has been scraping these sites for several months to mine the data publicly shared there. The data he observed included credit card numbers social security numbers, cracked Wi-Fi passwords, username and password dumps, chat logs, etc.

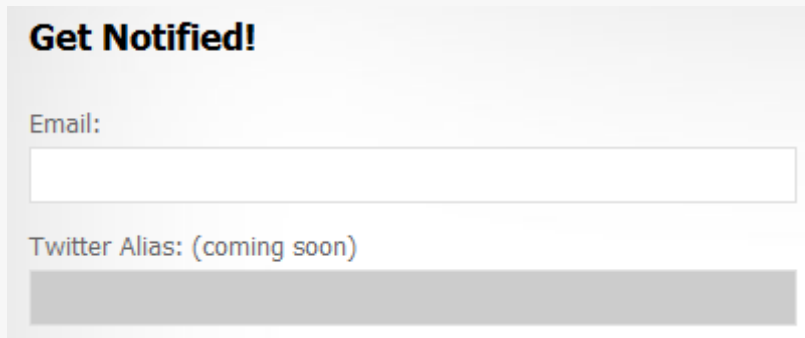
```
1 #!/usr/bin/perl
2 #####
3 #
4 # / \ / \ / \ / \ / \ / \ / \
5 # ( P | a | s | t | e | b | i | n )
6 # \ / \ / \ / \ / \ / \ / \
7 #
8 # / \ / \ / \ / \ / \ / \ / \
9 # ( S | c | r | a | p | e | r ) v4.0
10 # \ / \ / \ / \ / \ / \ / \
```

Scraping and archiving contents might be attractive for an organization conducting a lot of penetration tests, but might be an overkill for many testers. If searching local archives of these sites isn't practical for you, you can examine these sites for the data relevant to your target using their respective search tools or your favorite search engine (e.g., search Google for *password example.org site:pastebin.com*)

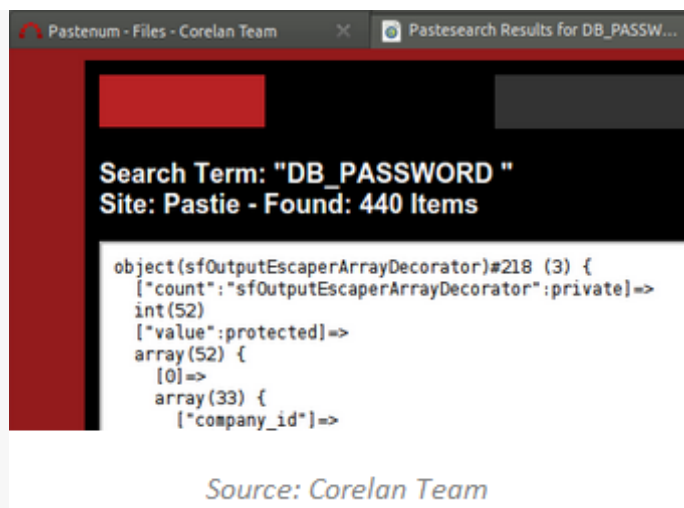
An alternative to Google is a specialized web-based search tool created by Andrew Mohawk called [Pastebin Parser](#). It lets you enter a query, which it runs against several pastebin sites [using a variety of techniques](#). Andrew also makes the tool available for download, if you want to install it locally and customize it for your needs.

A screenshot of a web interface with a black background. At the top, there is a white text input field containing the placeholder text "Enter Search Term Here..." and a small grey button with the word "search" in white. Below the input field, the text "About Pastebin Parser" is displayed in a yellow, monospaced font.

Andrew also makes available a web tool called [PasteLert](#), which allows you to set up alerts, so you get notified when the monitored pastebin sites publish content that matches the desired keywords.

A screenshot of a web form titled "Get Notified!" in bold black text. Below the title, there is a label "Email:" followed by a white text input field. Below that, there is a label "Twitter Alias: (coming soon)" followed by a greyed-out text input field.

The idea of mining pastebin data for penetration testing reconnaissance was initially discussed by the Corelan Team, who provides a free tool called [Pastenum](#) that you can install locally to query several pastebin sites.



As you can see, there are several ways of mining public text sites for data that might be useful during the reconnaissance stage of a penetration test. Consider adding the sites and utilities mentioned above to your assessment toolkit. And if you come across or write additional tools for this purpose, please leave a comment.

Updated March 16, 2015

DID YOU LIKE THIS?

Follow me for more of the good stuff.



TWITTER



RSS FEED



NEWSLETTER

About the Author

Lenny Zeltser develops teams, products, and programs that use information security to achieve business results. Over the past two decades, Lenny has been leading efforts to establish resilient security practices and solve hard security problems. As a respected author and speaker, he has been advancing cybersecurity tradecraft and contributing to the community. His insights build upon 20 years of real-world experiences, a Computer Science degree from the University of Pennsylvania, and an MBA degree from MIT Sloan.

[Learn more](#)

Copyright © 1995-2019 Lenny Zeltser. All rights reserved.