UNIX VS WEB PENTESTING

COMBINING SMALL BUILDING BLOCKS WITH PIPES

silent signal

András Veres-Szentkirályi 2019-07-26

$ whoami

András Veres-Szentkirályi

- OSCP, GWAPT, SISE
- Silent Signal co-founder
- pentester, toolmaker

Fahrplan

1. Burp
2. Making a difference
3. Format C:
4. B2B, C2C, P2P, E2E
5. No comment
6. Implementation details

Why Burp Suite

- `https://portswigger.net/`
- gold standard for web pentesting
- closed source (but extensible, see later)
- community edition is free
- pro is reasonably priced
- all-in-one: proxy, scanner, repeater ...

Alternatives to Burp

- OWASP ZAP (`https://www.owasp.org/index.php/ZAP`)
- mitmproxy (`https://mitmproxy.org/`)
- free in both senses
- also extensible (see later)
- nice ideas
- less polish

Extensibility

	Burp Extender	**mitmproxy**	**Piper**
Programming language(s)	JVM: Java, Kotlin, Jython, JRuby …	Python 3	∀
Development cycle	slow	fast	fast
Composability	low	low	high

This matters, since **pentesting is all about improvization and one-off solutions**.

Language of choice

- Jython: worst of both worlds
- JRuby: same as Jython
- Java: I still don’t like it
- Kotlin: better syntax at least
- `https://kotlinlang.org/docs/reference/comparison-to-java.html`

Fahrplan

Why not Burp Comparer

- Comparer has both text (“words”) and binary (“bytes”) diff support
- go find the differing parts yourself
- *Sync views* checkbox helps, but not much: no word-wrap, 2D scrollbar
- no option for c14n (see later)

Better text diff: git diff

- can be used outside Git repositories
- can do everything GNU diff does
- `--color=always`
- `-w`, `--ignore-all-space`
- `--color-words`

Better bin diff: vbindiff

- `https://www.cjmweb.net/vbindiff/`
- `apt install vbindiff`
- ↑ ↓ behave as expected
- ↲ jumps to the next difference
- behaves as a hex viewer upon loading a single file

Better bin diff: radiff2

- `https://r2wiki.readthedocs.io/en/latest/tools/radiff2/`
- `apt install radare2`
- nice ANSI colors
- it can do everything

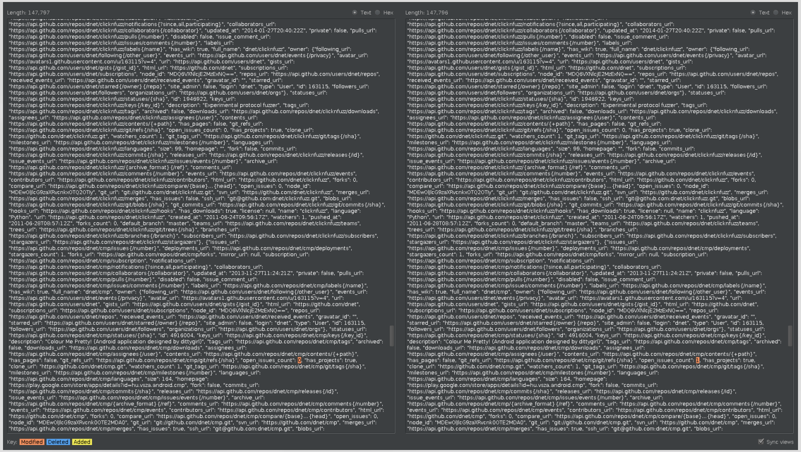
Better bin diff: flowdiff

- `https://github.com/dnet/flowtools/blob/master/bindiff.py`
- my own little diff (although originally made for a different purpose)
- useful for diffing more $n > 2$ files
- nice ANSI colors

A series of pipes

- pipes in Unix are great for combining small blocks
- what if we used c14n transformations before diffing?
- it has its own challenges
  - What combinations should be offered?
  - What’s the ideal GUI for presenting this?
  - Where’s the optimum between automation and manual config?

Comparison: Burp text diff



Length: 147,797 ● Text ○ Hex

```
"https://api.github.com/repos/dnet/clicknfuzz/notifications{?since,all,participating}", "collaborators_url":
"https://api.github.com/repos/dnet/clicknfuzz/collaborators{/collaborator}", "updated_at": "2014-01-27T20:40:22Z", "private": false, "pulls_url":
"https://api.github.com/repos/dnet/clicknfuzz/pulls{/number}", "disabled": false, "issue_comment_url":
"https://api.github.com/repos/dnet/clicknfuzz/issues/comments{/number}", "labels_url":
"https://api.github.com/repos/dnet/clicknfuzz/labels{/name}", "has_wiki": true, "full_name": "dnet/clicknfuzz", "owner": {"following_url":
"https://api.github.com/users/dnet/following{/other_user}", "events_url": "https://api.github.com/users/dnet/events{/privacy}", "avatar_url":
"https://avatars1.githubusercontent.com/u/163115?v=4", "url": "https://api.github.com/users/dnet", "gists_url":
"https://api.github.com/users/dnet/gists{/gist_id}", "html_url": "https://github.com/dnet", "subscriptions_url":
"https://api.github.com/users/dnet/subscriptions", "node_id": "MDQ6VXNlcjE2MzExNQ==", "repos_url": "https://api.github.com/users/dnet/repos",
"received_events_url": "https://api.github.com/users/dnet/received_events", "gravatar_id": "", "starred_url":
"https://api.github.com/users/dnet/starred{/owner}{/repo}", "site_admin": false, "login": "dnet", "type": "User", "id": 163115, "followers_url":
"https://api.github.com/users/dnet/followers", "organizations_url": "https://api.github.com/users/dnet/orgs"}, "statuses_url":
"https://api.github.com/repos/dnet/clicknfuzz/statuses/{sha}", "id": 1946922, "keys_url":
"https://api.github.com/repos/dnet/clicknfuzz/keys{/key_id}", "description": "Experimental protocol fuzzer", "tags_url":
"https://api.github.com/repos/dnet/clicknfuzz/tags", "archived": false, "downloads_url": "https://api.github.com/repos/dnet/clicknfuzz/downloads",
"assignees_url": "https://api.github.com/repos/dnet/clicknfuzz/assignees{/user}", "contents_url":
"https://api.github.com/repos/dnet/clicknfuzz/contents/{+path}", "has_pages": false, "git_refs_url":
"https://api.github.com/repos/dnet/clicknfuzz/git/refs{/sha}", "open_issues_count": 0, "has_projects": true, "clone_url":
"https://github.com/dnet/clicknfuzz.git", "watchers_count": 1, "git_tags_url": "https://api.github.com/repos/dnet/clicknfuzz/git/tags{/sha}",
"milestones_url": "https://api.github.com/repos/dnet/clicknfuzz/milestones{/number}", "languages_url":
"https://api.github.com/repos/dnet/clicknfuzz/languages", "size": 99, "homepage": "", "fork": false, "commits_url":
"https://api.github.com/repos/dnet/clicknfuzz/commits{/sha}", "releases_url": "https://api.github.com/repos/dnet/clicknfuzz/releases{/id}",
"issue_events_url": "https://api.github.com/repos/dnet/clicknfuzz/issues/events{/number}", "archive_url":
"https://api.github.com/repos/dnet/clicknfuzz/{archive_format}{/ref}", "comments_url":
"https://api.github.com/repos/dnet/clicknfuzz/comments{/number}", "events_url": "https://api.github.com/repos/dnet/clicknfuzz/events",
"contributors_url": "https://api.github.com/repos/dnet/clicknfuzz/contributors", "html_url": "https://github.com/dnet/clicknfuzz", "forks": 0,
"compare_url": "https://api.github.com/repos/dnet/clicknfuzz/compare/{base}...{head}", "open_issues": 0, "node_id":
"MDEwOlJlcG9zaXRvcnkxOTQ2OTIy", "git_url": "git://github.com/dnet/clicknfuzz.git", "svn_url": "https://github.com/dnet/clicknfuzz", "merges_url":
"https://api.github.com/repos/dnet/clicknfuzz/merges", "has_issues": false, "ssh_url": "git@github.com:dnet/clicknfuzz.git", "blobs_url":
"https://api.github.com/repos/dnet/clicknfuzz/git/blobs{/sha}", "git_commits_url": "https://api.github.com/repos/dnet/clicknfuzz/git/commits{/sha}",
"hooks_url": "https://api.github.com/repos/dnet/clicknfuzz/hooks", "has_downloads": true, "license": null, "name": "clicknfuzz", "language":
"Python", "url": "https://api.github.com/repos/dnet/clicknfuzz", "created_at": "2011-06-24T09:56:17Z", "watchers": 1, "pushed_at":
"2011-06-28T08:57:12Z", "forks_count": 0, "default_branch": "master", "teams_url": "https://api.github.com/repos/dnet/clicknfuzz/teams",
"trees_url": "https://api.github.com/repos/dnet/clicknfuzz/git/trees{/sha}", "branches_url":
"https://api.github.com/repos/dnet/clicknfuzz/branches{/branch}", "subscribers_url": "https://api.github.com/repos/dnet/clicknfuzz/subscribers",
"stargazers_url": "https://api.github.com/repos/dnet/clicknfuzz/stargazers"}, {"issues_url":
"https://api.github.com/repos/dnet/cmp/issues{/number}", "deployments_url": "https://api.github.com/repos/dnet/cmp/deployments",
"stargazers_count": 1, "forks_url": "https://api.github.com/repos/dnet/cmp/forks", "mirror_url": null, "subscription_url":
"https://api.github.com/repos/dnet/cmp/subscription", "notifications_url":
"https://api.github.com/repos/dnet/cmp/notifications{?since,all,participating}", "collaborators_url":
"https://api.github.com/repos/dnet/cmp/collaborators{/collaborator}", "updated_at": "2013-11-27T11:24:21Z", "private": false, "pulls_url":
"https://api.github.com/repos/dnet/cmp/pulls{/number}", "disabled": false, "issue_comment_url":
"https://api.github.com/repos/dnet/cmp/issues/comments{/number}", "labels_url": "https://api.github.com/repos/dnet/cmp/labels{/name}",
"has_wiki": true, "full_name": "dnet/cmp", "owner": {"following_url": "https://api.github.com/users/dnet/following{/other_user}", "events_url":
"https://api.github.com/users/dnet/events{/privacy}", "avatar_url": "https://avatars1.githubusercontent.com/u/163115?v=4", "url":
"https://api.github.com/users/dnet", "gists_url": "https://api.github.com/users/dnet/gists{/gist_id}", "html_url": "https://github.com/dnet",
"subscriptions_url": "https://api.github.com/users/dnet/subscriptions", "node_id": "MDQ6VXNlcjE2MzExNQ==", "repos_url":
"https://api.github.com/users/dnet/repos", "received_events_url": "https://api.github.com/users/dnet/received_events", "gravatar_id": "",
"starred_url": "https://api.github.com/users/dnet/starred{/owner}{/repo}", "site_admin": false, "login": "dnet", "type": "User", "id": 163115,
"followers_url": "https://api.github.com/users/dnet/followers", "organizations_url": "https://api.github.com/users/dnet/orgs"}, "statuses_url":
"https://api.github.com/repos/dnet/cmp/statuses/{sha}", "id": 4916004, "keys_url": "https://api.github.com/repos/dnet/cmp/keys{/key_id}",
"description": "Colour Me Pretty! (Android application designed by dittygirl)", "tags_url": "https://api.github.com/repos/dnet/cmp/tags", "archived":
false, "downloads_url": "https://api.github.com/repos/dnet/cmp/downloads", "assignees_url":
"https://api.github.com/repos/dnet/cmp/assignees{/user}", "contents_url": "https://api.github.com/repos/dnet/cmp/contents/{+path}",
"has_pages": false, "git_refs_url": "https://api.github.com/repos/dnet/cmp/git/refs{/sha}", "open_issues_count": 0, "has_projects": true,
"clone_url": "https://github.com/dnet/cmp.git", "watchers_count": 1, "git_tags_url": "https://api.github.com/repos/dnet/cmp/git/tags{/sha}",
"milestones_url": "https://api.github.com/repos/dnet/cmp/milestones{/number}", "languages_url":
"https://api.github.com/repos/dnet/cmp/languages", "size": 164, "homepage":
"https://play.google.com/store/apps/details?id=hu.vsza.android.cmp", "fork": false, "commits_url":
"https://api.github.com/repos/dnet/cmp/commits{/sha}", "releases_url": "https://api.github.com/repos/dnet/cmp/releases{/id}",
"issue_events_url": "https://api.github.com/repos/dnet/cmp/issues/events{/number}", "archive_url":
"https://api.github.com/repos/dnet/cmp/{archive_format}{/ref}", "comments_url": "https://api.github.com/repos/dnet/cmp/comments{/number}",
"events_url": "https://api.github.com/repos/dnet/cmp/events", "contributors_url": "https://api.github.com/repos/dnet/cmp/contributors", "html_url":
"https://github.com/dnet/cmp", "forks": 0, "compare_url": "https://api.github.com/repos/dnet/cmp/compare/{base}...{head}", "open_issues": 0,
"node_id": "MDEwOlJlcG9zaXRvcnk0OTE2MDA0", "git_url": "git://github.com/dnet/cmp.git", "svn_url": "https://github.com/dnet/cmp", "merges_url":
"https://api.github.com/repos/dnet/cmp/merges", "has_issues": true, "ssh_url": "git@github.com:dnet/cmp.git", "blobs_url":
```

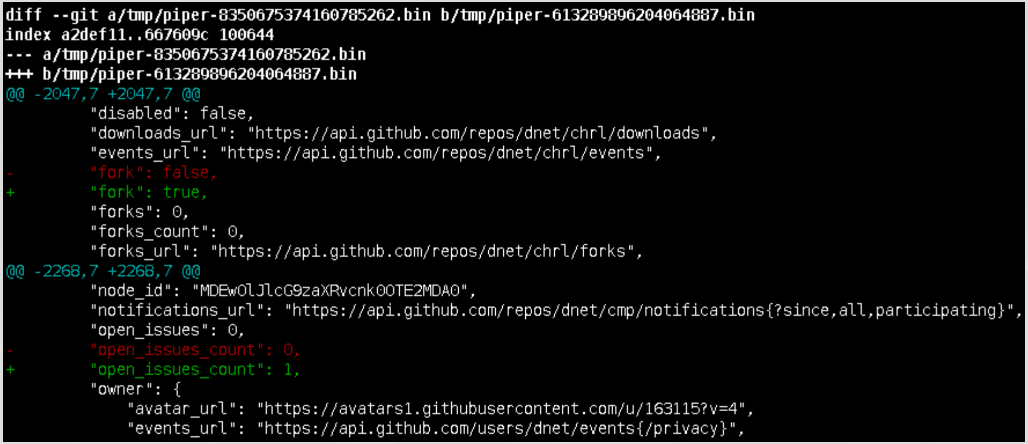
Key: Modified Deleted Added

Length: 147,796 ● Text ○ Hex

```
"https://api.github.com/repos/dnet/clicknfuzz/notifications{?since,all,participating}", "collaborators_url":
"https://api.github.com/repos/dnet/clicknfuzz/collaborators{/collaborator}", "updated_at": "2014-01-27T20:40:22Z", "private": false, "pulls_url":
"https://api.github.com/repos/dnet/clicknfuzz/pulls{/number}", "disabled": false, "issue_comment_url":
"https://api.github.com/repos/dnet/clicknfuzz/issues/comments{/number}", "labels_url":
"https://api.github.com/repos/dnet/clicknfuzz/labels{/name}", "has_wiki": true, "full_name": "dnet/clicknfuzz", "owner": {"following_url":
"https://api.github.com/users/dnet/following{/other_user}", "events_url": "https://api.github.com/users/dnet/events{/privacy}", "avatar_url":
"https://avatars1.githubusercontent.com/u/163115?v=4", "url": "https://api.github.com/users/dnet", "gists_url":
"https://api.github.com/users/dnet/gists{/gist_id}", "html_url": "https://github.com/dnet", "subscriptions_url":
"https://api.github.com/users/dnet/subscriptions", "node_id": "MDQ6VXNlcjE2MzExNQ==", "repos_url": "https://api.github.com/users/dnet/repos",
"received_events_url": "https://api.github.com/users/dnet/received_events", "gravatar_id": "", "starred_url":
"https://api.github.com/users/dnet/starred{/owner}{/repo}", "site_admin": false, "login": "dnet", "type": "User", "id": 163115, "followers_url":
"https://api.github.com/users/dnet/followers", "organizations_url": "https://api.github.com/users/dnet/orgs"}, "statuses_url":
"https://api.github.com/repos/dnet/clicknfuzz/statuses/{sha}", "id": 1946922, "keys_url":
"https://api.github.com/repos/dnet/clicknfuzz/keys{/key_id}", "description": "Experimental protocol fuzzer", "tags_url":
"https://api.github.com/repos/dnet/clicknfuzz/tags", "archived": false, "downloads_url": "https://api.github.com/repos/dnet/clicknfuzz/downloads",
"assignees_url": "https://api.github.com/repos/dnet/clicknfuzz/assignees{/user}", "contents_url":
"https://api.github.com/repos/dnet/clicknfuzz/contents/{+path}", "has_pages": false, "git_refs_url":
"https://api.github.com/repos/dnet/clicknfuzz/git/refs{/sha}", "open_issues_count": 0, "has_projects": true, "clone_url":
"https://github.com/dnet/clicknfuzz.git", "watchers_count": 1, "git_tags_url": "https://api.github.com/repos/dnet/clicknfuzz/git/tags{/sha}",
"milestones_url": "https://api.github.com/repos/dnet/clicknfuzz/milestones{/number}", "languages_url":
"https://api.github.com/repos/dnet/clicknfuzz/languages", "size": 99, "homepage": "", "fork": false, "commits_url":
"https://api.github.com/repos/dnet/clicknfuzz/commits{/sha}", "releases_url": "https://api.github.com/repos/dnet/clicknfuzz/releases{/id}",
"issue_events_url": "https://api.github.com/repos/dnet/clicknfuzz/issues/events{/number}", "archive_url":
"https://api.github.com/repos/dnet/clicknfuzz/{archive_format}{/ref}", "comments_url":
"https://api.github.com/repos/dnet/clicknfuzz/comments{/number}", "events_url": "https://api.github.com/repos/dnet/clicknfuzz/events",
"contributors_url": "https://api.github.com/repos/dnet/clicknfuzz/contributors", "html_url": "https://github.com/dnet/clicknfuzz", "forks": 0,
"compare_url": "https://api.github.com/repos/dnet/clicknfuzz/compare/{base}...{head}", "open_issues": 0, "node_id":
"MDEwOlJlcG9zaXRvcnkxOTQ2OTIy", "git_url": "git://github.com/dnet/clicknfuzz.git", "svn_url": "https://github.com/dnet/clicknfuzz", "merges_url":
"https://api.github.com/repos/dnet/clicknfuzz/merges", "has_issues": false, "ssh_url": "git@github.com:dnet/clicknfuzz.git", "blobs_url":
"https://api.github.com/repos/dnet/clicknfuzz/git/blobs{/sha}", "git_commits_url": "https://api.github.com/repos/dnet/clicknfuzz/git/commits{/sha}",
"hooks_url": "https://api.github.com/repos/dnet/clicknfuzz/hooks", "has_downloads": true, "license": null, "name": "clicknfuzz", "language":
"Python", "url": "https://api.github.com/repos/dnet/clicknfuzz", "created_at": "2011-06-24T09:56:17Z", "watchers": 1, "pushed_at":
"2011-06-28T08:57:12Z", "forks_count": 0, "default_branch": "master", "teams_url": "https://api.github.com/repos/dnet/clicknfuzz/teams",
"trees_url": "https://api.github.com/repos/dnet/clicknfuzz/git/trees{/sha}", "branches_url":
"https://api.github.com/repos/dnet/clicknfuzz/branches{/branch}", "subscribers_url": "https://api.github.com/repos/dnet/clicknfuzz/subscribers",
"stargazers_url": "https://api.github.com/repos/dnet/clicknfuzz/stargazers"}, {"issues_url":
"https://api.github.com/repos/dnet/cmp/issues{/number}", "deployments_url": "https://api.github.com/repos/dnet/cmp/deployments",
"stargazers_count": 1, "forks_url": "https://api.github.com/repos/dnet/cmp/forks", "mirror_url": null, "subscription_url":
"https://api.github.com/repos/dnet/cmp/subscription", "notifications_url":
"https://api.github.com/repos/dnet/cmp/notifications{?since,all,participating}", "collaborators_url":
"https://api.github.com/repos/dnet/cmp/collaborators{/collaborator}", "updated_at": "2013-11-27T11:24:21Z", "private": false, "pulls_url":
"https://api.github.com/repos/dnet/cmp/pulls{/number}", "disabled": false, "issue_comment_url":
"https://api.github.com/repos/dnet/cmp/issues/comments{/number}", "labels_url": "https://api.github.com/repos/dnet/cmp/labels{/name}",
"has_wiki": true, "full_name": "dnet/cmp", "owner": {"following_url": "https://api.github.com/users/dnet/following{/other_user}", "events_url":
"https://api.github.com/users/dnet/events{/privacy}", "avatar_url": "https://avatars1.githubusercontent.com/u/163115?v=4", "url":
"https://api.github.com/users/dnet", "gists_url": "https://api.github.com/users/dnet/gists{/gist_id}", "html_url": "https://github.com/dnet",
"subscriptions_url": "https://api.github.com/users/dnet/subscriptions", "node_id": "MDQ6VXNlcjE2MzExNQ==", "repos_url":
"https://api.github.com/users/dnet/repos", "received_events_url": "https://api.github.com/users/dnet/received_events", "gravatar_id": "",
"starred_url": "https://api.github.com/users/dnet/starred{/owner}{/repo}", "site_admin": false, "login": "dnet", "type": "User", "id": 163115,
"followers_url": "https://api.github.com/users/dnet/followers", "organizations_url": "https://api.github.com/users/dnet/orgs"}, "statuses_url":
"https://api.github.com/repos/dnet/cmp/statuses/{sha}", "id": 4916004, "keys_url": "https://api.github.com/repos/dnet/cmp/keys{/key_id}",
"description": "Colour Me Pretty! (Android application designed by dittygirl)", "tags_url": "https://api.github.com/repos/dnet/cmp/tags", "archived":
false, "downloads_url": "https://api.github.com/repos/dnet/cmp/downloads", "assignees_url":
"https://api.github.com/repos/dnet/cmp/assignees{/user}", "contents_url": "https://api.github.com/repos/dnet/cmp/contents/{+path}",
"has_pages": false, "git_refs_url": "https://api.github.com/repos/dnet/cmp/git/refs{/sha}", "open_issues_count": 1, "has_projects": true,
"clone_url": "https://github.com/dnet/cmp.git", "watchers_count": 1, "git_tags_url": "https://api.github.com/repos/dnet/cmp/git/tags{/sha}",
"milestones_url": "https://api.github.com/repos/dnet/cmp/milestones{/number}", "languages_url":
"https://api.github.com/repos/dnet/cmp/languages", "size": 164, "homepage":
"https://play.google.com/store/apps/details?id=hu.vsza.android.cmp", "fork": false, "commits_url":
"https://api.github.com/repos/dnet/cmp/commits{/sha}", "releases_url": "https://api.github.com/repos/dnet/cmp/releases{/id}",
"issue_events_url": "https://api.github.com/repos/dnet/cmp/issues/events{/number}", "archive_url":
"https://api.github.com/repos/dnet/cmp/{archive_format}{/ref}", "comments_url": "https://api.github.com/repos/dnet/cmp/comments{/number}",
"events_url": "https://api.github.com/repos/dnet/cmp/events", "contributors_url": "https://api.github.com/repos/dnet/cmp/contributors", "html_url":
"https://github.com/dnet/cmp", "forks": 0, "compare_url": "https://api.github.com/repos/dnet/cmp/compare/{base}...{head}", "open_issues": 0,
"node_id": "MDEwOlJlcG9zaXRvcnk0OTE2MDA0", "git_url": "git://github.com/dnet/cmp.git", "svn_url": "https://github.com/dnet/cmp", "merges_url":
"https://api.github.com/repos/dnet/cmp/merges", "has_issues": true, "ssh_url": "git@github.com:dnet/cmp.git", "blobs_url":
```

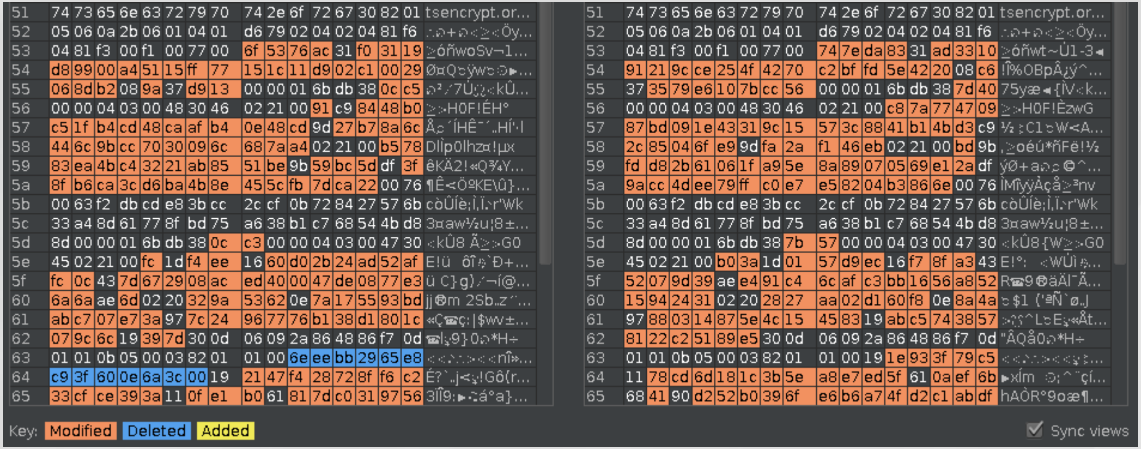
✓ Sync views

Comparison: Python + git diff



```
diff --git a/tmp/piper-8350675374160785262.bin b/tmp/piper-6132898962040648887.bin
index a2def11..667609c 100644
--- a/tmp/piper-8350675374160785262.bin
+++ b/tmp/piper-6132898962040648887.bin
@@ -2047,7 +2047,7 @@
          "disabled": false,
          "downloads_url": "https://api.github.com/repos/dnet/chrl/downloads",
          "events_url": "https://api.github.com/repos/dnet/chrl/events",
-         "fork": false,
+         "fork": true,
          "forks": 0,
          "forks_count": 0,
          "forks_url": "https://api.github.com/repos/dnet/chrl/forks",
@@ -2268,7 +2268,7 @@
          "node_id": "MDEwOlJlcG9zaXRvcnk0OTE2MDA0",
          "notifications_url": "https://api.github.com/repos/dnet/cmp/notifications{?since,all,participating}",
          "open_issues": 0,
-         "open_issues_count": 0,
+         "open_issues_count": 1,
          "owner": {
              "avatar_url": "https://avatars1.githubusercontent.com/u/163115?v=4",
              "events_url": "https://api.github.com/users/dnet/events{/privacy}",
```

Comparison: Burp binary diff



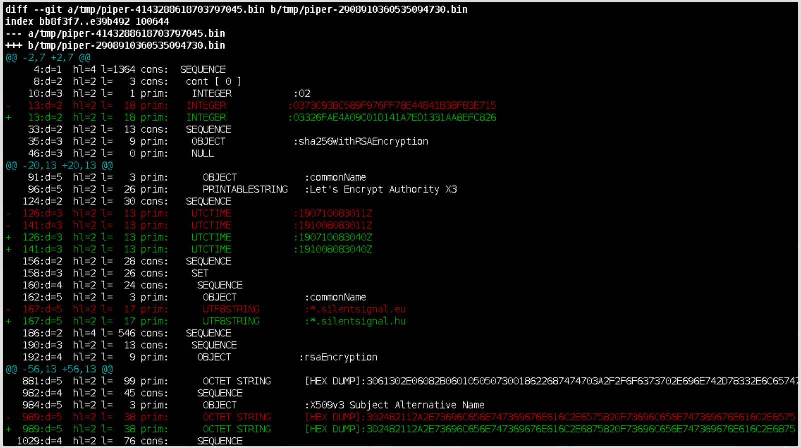
```
51  74 73 65 6e 63 72 79 70  74 2e 6f 72 67 30 82 01  tsencrypt.or...
52  05 06 0a 2b 06 01 04 01  d6 79 02 04 02 04 81 f6  ::+:<≥<Öy...
53  04 81 f3 00 f1 00 77 00  6f 53 76 ac 31 f0 31 19  ≥óñwoSv¬1...
54  d8 99 00 a4 51 15 ff 77  15 1c 11 d9 02 c1 00 29  Ø¤Q:ÿw::▶...
55  06 8d b2 08 9a 37 d9 13  00 00 01 6b db 38 0c c5  :²/7Ù:<kÛ...
56  00 00 04 03 00 48 30 46  02 21 00 91 c9 84 48 b0  ≥:H0F!ÉH°
57  c5 1f b4 cd 48 ca af b4  0e 48 cd 9d 27 b7 8a 6c  Å:´ÍHÊ¯´.HÍ'·l
58  44 6c 9b cc 70 30 09 6c  68 7a a4 02 21 00 b5 78  DlÌp0lhz¤!µx
59  83 ea 4b c4 32 21 ab 85  51 be 9b 59 bc 5d df 3f  êKÄ2!«Q¾Y...
5a  8f b6 ca 3c d6 ba 4b 8e  45 5c fb 7d ca 22 00 76  ¶Ê<ÖºKE\û}...
5b  00 63 f2 db cd e8 3b cc  2c cf 0b 72 84 27 57 6b  còÛÍè;Ì,Ï:r'Wk
5c  33 a4 8d 61 77 8f bd 75  a6 38 b1 c7 68 54 4b d8  3¤aw½u¦8±...
5d  8d 00 00 01 6b db 38 0c  c3 00 00 04 03 00 47 30  <kÛ8 Ã≥:G0
5e  45 02 21 00 fc 1d f4 ee  16 60 d0 2b 24 ad 52 af  E!ü ôî:`Ð+...
5f  fc 0c 43 7d 67 29 08 ac  ed 40 00 47 de 08 77 e3  ü C}g)/¬í@...
60  6a 6a ae 6d 02 20 32 9a  53 62 0e 7a 17 55 93 bd  jj®m 2Sb.z´¨...
61  ab c7 07 e7 3a 97 7c 24  96 77 76 b1 38 d1 80 1c  «Ç☎ç:|$wv±...
62  07 9c 6c 19 39 7d 30 0d  06 09 2a 86 48 86 f7 0d  ☎l:9}0:*H÷
63  01 01 0b 05 00 03 82 01  01 00 6e ee bb 29 65 e8  <<::><<nî»...
64  c9 3f 60 0e 6a 3c 00 19  21 47 f4 28 72 8f f6 c2  É?`.j<:!Gô(r...
65  33 cf ce 39 3a 11 0f e1  b0 61 81 7d c0 31 97 56  3ÏÎ9:▶:á°a}...
```

```
51  74 73 65 6e 63 72 79 70  74 2e 6f 72 67 30 82 01  tsencrypt.or...
52  05 06 0a 2b 06 01 04 01  d6 79 02 04 02 04 81 f6  ::+:<≥<Öy...
53  04 81 f3 00 f1 00 77 00  74 7e da 83 31 ad 33 10  ≥óñwt~Ú1-3◀
54  91 21 9c ce 25 4f 42 70  c2 bf fd 5e 42 20 08 c6  !Î%OBpÂ¿ý^...
55  37 35 79 e6 10 7b cc 56  00 00 01 6b db 38 7d 40  75yæ◀{ÌV<k...
56  00 00 04 03 00 48 30 46  02 21 00 c8 7a 77 47 09  ≥:H0F!ÈzwG
57  87 bd 09 1e 43 31 9c 15  57 3c 88 41 b1 4b d3 c9  ½:C1:W<A...
58  2c 85 04 6f e9 9d fa 2a  f1 46 eb 02 21 00 bd 9b  ,≥oéú*ñFë!½
59  fd d8 2b 61 06 1f a9 5e  8a 89 07 05 69 e1 2a df  ýØ+a::©^...
5a  9a cc 4d ee 79 ff c0 e7  e5 82 04 b3 86 6e 00 76  ÌMîyÿÀçå≥³nv
5b  00 63 f2 db cd e8 3b cc  2c cf 0b 72 84 27 57 6b  còÛÍè;Ì,Ï:r'Wk
5c  33 a4 8d 61 77 8f bd 75  a6 38 b1 c7 68 54 4b d8  3¤aw½u¦8±...
5d  8d 00 00 01 6b db 38 7b  57 00 00 04 03 00 47 30  <kÛ8{W≥:G0
5e  45 02 21 00 b0 3a 1d 01  57 d9 ec 16 f7 8f a3 43  E!°:  <WÙì:...
5f  52 07 9d 39 ae e4 91 c4  6c af c3 bb 16 56 a8 52  R☎9®äÄl¯Ã...
60  15 94 24 31 02 20 28 27  aa 02 d1 60 f8 0e 8a 4a  :$1 ('ªÑ`ø.J
61  97 88 03 14 87 5e 4c 15  45 83 19 ab c5 74 38 57  :::^L:E:«Åt...
62  81 22 c2 51 89 e5 30 0d  06 09 2a 86 48 86 f7 0d  "ÂQå0:*H÷
63  01 01 0b 05 00 03 82 01  01 00 19 1e 93 3f 79 c5  <<::><<::...
64  11 78 cd 6d 18 1c 3b 5e  a8 e7 ed 5f 61 0a ef 6b  ▶xÍm :;^¨çí...
65  68 41 90 d2 52 b0 39 6f  e6 b6 a7 4f d2 c1 ab df  hAÒR°9oæ¶...
```

Key: 🟧 Modified 🟦 Deleted 🟨 Added

☑ Sync views

Comparison: OpenSSL + git diff



```
diff --git a/tmp/piper-4143288618703797045.bin b/tmp/piper-2908910360535094730.bin
index bb8f3f7..e39b492 100644
--- a/tmp/piper-4143288618703797045.bin
+++ b/tmp/piper-2908910360535094730.bin
@@ -2,7 +2,7 @@
     4:d=1  hl=4 l=1364 cons:  SEQUENCE
     8:d=2  hl=2 l=   3 cons:   cont [ 0 ]
    10:d=3  hl=2 l=   1 prim:    INTEGER           :02
-   13:d=2  hl=2 l=  18 prim:   INTEGER           :0373C93BC589F976FF78E44B41B38FB3E715
+   13:d=2  hl=2 l=  18 prim:   INTEGER           :03326FAE4A09C01D141A7ED1331AA8EFC826
    33:d=2  hl=2 l=  13 cons:   SEQUENCE
    35:d=3  hl=2 l=   9 prim:    OBJECT            :sha256WithRSAEncryption
    46:d=3  hl=2 l=   0 prim:    NULL
@@ -20,13 +20,13 @@
    91:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
    96:d=5  hl=2 l=  26 prim:      PRINTABLESTRING   :Let's Encrypt Authority X3
   124:d=2  hl=2 l=  30 cons:   SEQUENCE
-  126:d=3  hl=2 l=  13 prim:    UTCTIME           :190710083011Z
-  141:d=3  hl=2 l=  13 prim:    UTCTIME           :191008083011Z
+  126:d=3  hl=2 l=  13 prim:    UTCTIME           :190710083040Z
+  141:d=3  hl=2 l=  13 prim:    UTCTIME           :191008083040Z
   156:d=2  hl=2 l=  28 cons:   SEQUENCE
   158:d=3  hl=2 l=  26 cons:    SET
   160:d=4  hl=2 l=  24 cons:     SEQUENCE
   162:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
-  167:d=5  hl=2 l=  17 prim:      UTF8STRING        :*.silentsignal.eu
+  167:d=5  hl=2 l=  17 prim:      UTF8STRING        :*.silentsignal.hu
   186:d=2  hl=4 l= 546 cons:   SEQUENCE
   190:d=3  hl=2 l=  13 cons:    SEQUENCE
   192:d=4  hl=2 l=   9 prim:     OBJECT            :rsaEncryption
@@ -56,13 +56,13 @@
   881:d=5  hl=2 l=  99 prim:      OCTET STRING      [HEX DUMP]:3061302E06082B0601050507300186226874747470 3A2F2F6F6373702E696E742D78332E6C65747
   982:d=4  hl=2 l=  45 cons:     SEQUENCE
   984:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Subject Alternative Name
-  989:d=5  hl=2 l=  38 prim:      OCTET STRING      [HEX DUMP]:302482112A2E73696C656E747369676E616C2E6575820F73696C656E747369676E616C2E6575
+  989:d=5  hl=2 l=  38 prim:      OCTET STRING      [HEX DUMP]:302482112A2E73696C656E747369676E616C2E6875820F73696C656E747369676E616C2E6875
  1029:d=4  hl=2 l=  76 cons:     SEQUENCE
```

Implementation

Request(s) / Response(s) 〉 $n \in limits$ 〉 filter *(optional)* 〉 `./command --param ...` 〉 window *(optional)*

- number of inputs can be limited min/max (both can be omitted)
  - viewer: $n = 1$
  - diff: $n = 2$ or even $n \geq 2$
- filter: if present and doesn't match, hide command
- window can be
  - no window for commands with their own GUI
  - simple text window
  - limited terminal emulator that can handle ANSI color sequences

Fahrplan

1. Burp
2. Making a difference
3. Format C:
4. B2B, C2C, P2P, E2E
5. No comment
6. Implementation details

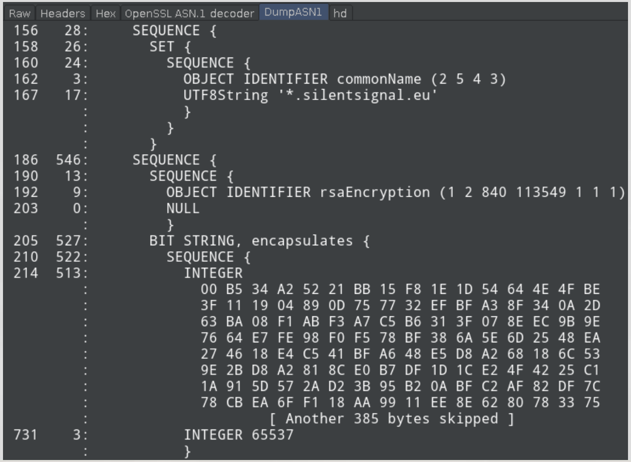
Why not Burp Proxy et al

- Built-in raw, params (URL encoded), headers, hex, HTML, XML, AMF, .NET
- What about
  - JSON (weird relationship)
  - ASN.1 / DER
  - Protocol Buffers
- there are purpose-build message editors for some, while not for others

ASN.1 / DER

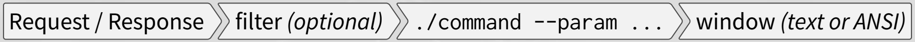
- used in more and more APIs
- certificates, public and private keys, CSRs, CRLs
- easy to spot based on the first two octets being `{0x30, 0x82}` or `{0x30, 0x80}`
- OpenSSL FTW: `man asn1parse`
- `dumpasn1` is also nice (Debian/Ubuntu package has the same name)

Example: DumpASN1 in Piper



```
 156   28:     SEQUENCE {
 158   26:       SET {
 160   24:         SEQUENCE {
 162    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 167   17:           UTF8String '*.silentsignal.eu'
         :           }
         :         }
         :       }
 186  546:     SEQUENCE {
 190   13:       SEQUENCE {
 192    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
 203    0:         NULL
         :         }
 205  527:       BIT STRING, encapsulates {
 210  522:         SEQUENCE {
 214  513:           INTEGER
         :             00 B5 34 A2 52 21 BB 15 F8 1E 1D 54 64 4E 4F BE
         :             3F 11 19 04 89 0D 75 77 32 EF BF A3 8F 34 0A 2D
         :             63 BA 08 F1 AB F3 A7 C5 B6 31 3F 07 8E EC 9B 9E
         :             76 64 E7 FE 98 F0 F5 78 BF 38 6A 5E 6D 25 48 EA
         :             27 46 18 E4 C5 41 BF A6 48 E5 D8 A2 68 18 6C 53
         :             9E 2B D8 A2 81 8C E0 B7 DF 1D 1C E2 4F 42 25 C1
         :             1A 91 5D 57 2A D2 3B 95 B2 0A BF C2 AF 82 DF 7C
         :             78 CB EA 6F F1 18 AA 99 11 EE 8E 62 80 78 33 75
         :                     [ Another 385 bytes skipped ]
 731    3:           INTEGER 65537
         :           }
```

Implementation



- single input
- read only for now
- filter: if present and doesn't match, hide message editor
- window can be either
  - simple text window or
  - limited terminal emulator that can handle ANSI color sequences

Fahrplan

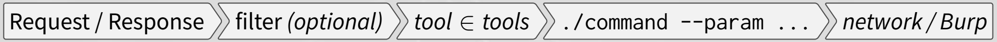
Why not Scanner (in itself)

- OAuth 1: signature in HTTP header based on all parameters **and** a *nonce*
- WS-Security: XML signature based on body, which can include a *nonce*
- End-to-end encryption is getting deployed in more and more places
- Nice idea: Brida
  - Source code: `https://github.com/federicodotta/Brida`
  - `https://techblog.mediaservice.net/2018/04/brida-a-step-by-step-user-guide/`

E2E a'la Piper

- modify client to use our public key
- now we can decrypt with a custom message viewer
- (re)encrypt with server public key
  - proxy: decrypt with our own, encrypt with server's
  - scanner et al: just encrypt with server key
- Burp offers HTTP listeners for this purpose

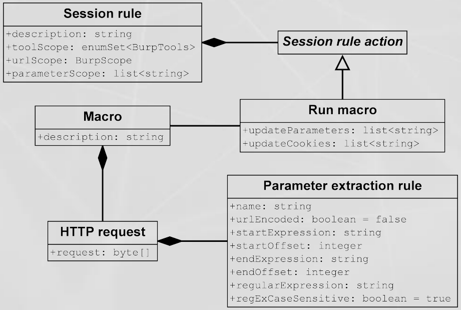
Implementation



- single input (can be request or response but not both)
- filter: if present and doesn’t match, ignore item
- tool: can be narrowed to e.g. $\{scanner, intruder\}$
- requests go towards the network with modifications applied
- responses go towards Burp with modifications applied

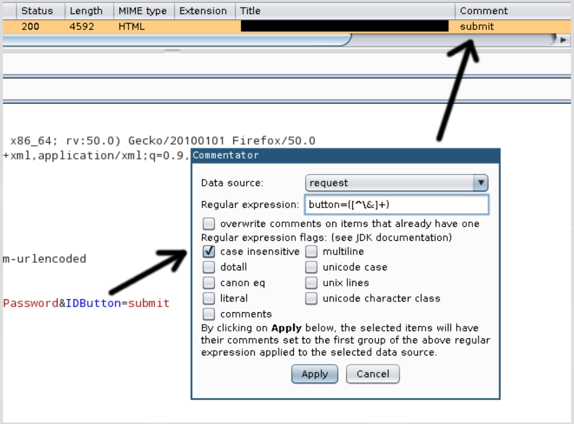
What about Macros

- similar to HTTP listener for requests
- difference: modifications are “backported” to request in *repeater*
- difference: can be integrated into Burp’s session handling rules


Session rule
+description: string
+toolScope: enumSet<BurpTools>
+urlScope: BurpScope
+parameterScope: list<string>
Session rule action
Macro
+description: string
Run macro
+updateParameters: list<string>
+updateCookies: list<string>
HTTP request
+request: byte[]
Parameter extraction rule
+name: string
+urlEncoded: boolean = false
+startExpression: string
+startOffset: integer
+endExpression: string
+endOffset: integer
+regularExpression: string
+regExCaseSensitive: boolean = true

Fahrplan

Prior art: commentator



Status	Length	MIME type	Extension	Title	Comment
200	4592	HTML		[redacted]	submit

```
x86_64; rv:50.0) Gecko/20100101 Firefox/50.0
+xml,application/xml;q=0.9,
m-urlencoded
Password&IDButton=submit
```

Commentator

Data source: request

Regular expression: button=([^\&]+)

☐ overwrite comments on items that already have one

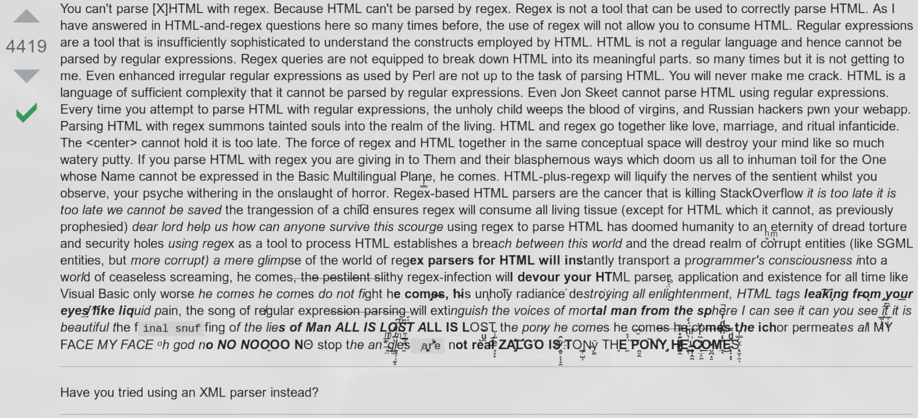
Regular expression flags: (see JDK documentation)

☑ case insensitive ☐ multiline
☐ dotall ☐ unicode case
☐ canon eq ☐ unix lines
☐ literal ☐ unicode character class
☐ comments

By clicking on **Apply** below, the selected items will have their comments set to the first group of the above regular expression applied to the selected data source.

https://github.com/silentsignal/burp-commentator

Why not regex



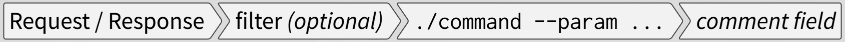
4419

You can't parse [X]HTML with regex. Because HTML can't be parsed by regex. Regex is not a tool that can be used to correctly parse HTML. As I have answered in HTML-and-regex questions here so many times before, the use of regex will not allow you to consume HTML. Regular expressions are a tool that is insufficiently sophisticated to understand the constructs employed by HTML. HTML is not a regular language and hence cannot be parsed by regular expressions. Regex queries are not equipped to break down HTML into its meaningful parts. so many times but it is not getting to me. Even enhanced irregular regular expressions as used by Perl are not up to the task of parsing HTML. You will never make me crack. HTML is a language of sufficient complexity that it cannot be parsed by regular expressions. Even Jon Skeet cannot parse HTML using regular expressions. Every time you attempt to parse HTML with regular expressions, the unholy child weeps the blood of virgins, and Russian hackers pwn your webapp. Parsing HTML with regex summons tainted souls into the realm of the living. HTML and regex go together like love, marriage, and ritual infanticide. The <center> cannot hold it is too late. The force of regex and HTML together in the same conceptual space will destroy your mind like so much watery putty. If you parse HTML with regex you are giving in to Them and their blasphemous ways which doom us all to inhuman toil for the One whose Name cannot be expressed in the Basic Multilingual Plane, he comes. HTML-plus-regexp will liquify the nerves of the sentient whilst you observe, your psyche withering in the onslaught of horror. Regex-based HTML parsers are the cancer that is killing StackOverflow *it is too late it is too late we cannot be saved* the trangession of a chi͡ld ensures regex will consume all living tissue (except for HTML which it cannot, as previously prophesied) *dear lord help us how can anyone survive this scourge* using regex to parse HTML has doomed humanity to an eternity of dread torture and security holes *using rege*x as a tool to process HTML establishes a brea*ch between this world* and the dread realm of c͒ͪo͛ͫrrupt entities (like SGML entities, but *more corrupt) a mere glimp*se of the world of reg**ex parsers for HTML will ins**tantly transport a p*rogrammer's consciousness i*nto a wor*l*d of ceaseless screaming, he comes~~, the pestilent s~~lithy regex-infection wil**l devour your HT**ML parser, application and existence for all time like Visual Basic only worse *he comes he comes do not fi*ght h**e com̡e̶s, ̕h̵i**s un̨ho͞ly radiańcé destro҉ying all enli̍̈́̂̈́ghtenment, HTML tags **lea͠ki̧n͘g fr̶ǫm ̡yo͟ur eye͢s̸ ̛l̕ik͏e liq**uid pain, the song of re̸gular expre~~ssion parsing~~ will exti*nguish the voices of mor***tal man from the sp***here I can see it can you see ̲͚̖͔̙î̩́t̲͎̩̱͔́̋̀ it is beautiful t*he f `inal snuf` fing *o*f the lie*s **of Man ALL IS LOŚ͖̩͇̗̪̏̈́T ALL I**S LOST the pon̷y he come*s he c̶̮omes ~~he co~~mes *t*he ich**or permeates al*l MY FACE MY FACE ᵒh god n**o NO NOO̼**O**O N**Θ stop t*he an*̶͑̾̾̅ͫ͏̙̤g͇̫͛͆̾ͫ̑͆l͖͉̗̩̳̟̍ͫͥͨe̠̅s ͎a̧͈͖r̽̾̈́͒͑e n**ot rè̑ͧ̌aͨl̘̝̙̃ͤ͂̾̆ ZA̡͊͠͝LGΌ ISͮ̂҉̯͈͕̹̘̱ TO͇̹̺ͅƝ̴ȳ̳ TH̘Ë͖́̉ ͠P̯͍̭O̚N̐Y̡ H̸̡̪̯ͨ͊̽̅̾̎Ȩ̬̩̾͛ͪ̈́̀́͘ ̶̧̨̱̹̭̯ͧ̾ͬC̷̙̲̝͖ͭ̏ͥͮ͟Oͮ͏̮̪̝͍M̲̖͊̒ͪͩͬ̚̚͜Ȇ̴̟̟͙̞ͩ͌͝S̨̥̫͎̭ͯ̿̔̀ͅ

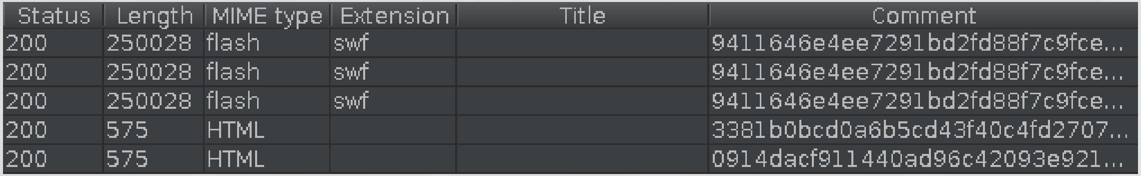
Have you tried using an XML parser instead?

https://stackoverflow.com/questions/1732348/regex-match-open-tags-except-xhtml-self-contained-tags/

Implementation



- single input
- filter: if present and doesn't match, ignore item
- overwriting previous comments can be disabled



Status	Length	MIME type	Extension	Title	Comment
200	250028	flash	swf		9411646e4ee7291bd2fd88f7c9fce...
200	250028	flash	swf		9411646e4ee7291bd2fd88f7c9fce...
200	250028	flash	swf		9411646e4ee7291bd2fd88f7c9fce...
200	575	HTML			3381b0bcd0a6b5cd43f40c4fd2707...
200	575	HTML			0914dacf911440ad96c42093e921...

Fahrplan

1. Burp
2. Making a difference
3. Format C:
4. B2B, C2C, P2P, E2E
5. No comment
6. Implementation details

Protocol Buffers

- developed by Google, released under BSD license
- generates nice code from IDL: immutable objects with builders
- compact and reasonably fast (de)serialization
- backward and forward compatible
- binary format is used to store config locally
  - `void saveExtensionSetting(String name, String value);`
  - `String loadExtensionSetting(String name);`
  - Configuration ❯ ProtoBuf binary wire format ❯ gzip ❯ Base85
  - `$HOME▸.java▸.userPrefs▸burp▸extensions▸<garbage>▸prefs.xml`

YAML Ain't Markup Language

- "human friendly data serialization standard" (`https://yaml.org/`)
- for sharing config snippets
- import/export skips certain attributes present in ProtoBuf
  - enabled/disabled
  - local config flags, such as developer mode

```
prefix: [python, -m, json.tool]
inputMethod: stdin
name: Python JSON formatter
filter:
  orElse:
    - {prefix: '{', postfix: '}'}
    - {prefix: '[', postfix: ']'}
```

Filters

- simple static prefix/postfix
- regular expression
- header match
  - for HTTP requests only
  - header name (case insensitive) + regex for value
- command match
  - exit code match
  - recursion: filter on stdout and/or stderr
- recursion: $0 \ldots \infty$ filters
  - $\vee$ (“or”) – at least one must match
  - $\wedge$ (“and”) – all must match
- negation for all of the above

Outro

- source code and binaries under GPL: `https://github.com/silentsignal/burp-piper`
- config GUI is kind of complete
- core functionality WORKSFORME
- pull requests welcome

THANKS!

ANDRÁS VERES-SZENTKIRÁLYI

vsza@silentsignal.hu

facebook.com/silentsignal.hu

@SilentSignalHU

@dn3t