1. Portswigger XSS Cheatsheet, OWASP Cheatsheet, XSS Vector Cheatsheet and many more dataset are collection of various techniques of XSS Payload in Plain Text format

```
cyss.txt

// cybody oninput=javascript:alert(1)><input autofocus>
// cybody oninput=javascript:javascript:alert(1)">CLICKME</math> cybody cybody>
// cybody cybody cybody>
// cybody cybody cybody>
// cybody cybod
```

2. CSIC Database contains Method, User-Agent, Pragma, Cache-Control, Accept, Accept-encoding, Accept-charset, language, host, cookie, content-type, URL. This dataset is nothing but a Client request info to a specific website where XSS payload found in URL parameter

Α	В	С	D	Е			F			(	3	Н	1	J	
	Method	User-Agen	Pragma	Cache-Cont	rol	Acce	pt		Accept	-encod	ling	Accept-ch	language	host	cookie
Normal	GET	Mozilla/5.0	no-cache	no-cache te		text/x	ml,application	on/xml,app	x-gzip,	x-defla	ate, gzip, def	la utf-8, utf-8	en :	localhost:8	JSESSION
Normal	GET	Mozilla/5.0	no-cache	no-cache		text/x	ml,application	on/xml,app	x-gzip,	x-defla	ate, gzip, def	la utf-8, utf-8	en :	localhost:8	JSESSION
Normal	POST	Mozilla/5.0	no-cache	no-cache		text/x	ml,application	on/xml,app	x-gzip,	x-defla	ate, gzip, def	la utf-8, utf-8	en :	localhost:8	JSESSION
Normal	GET	Mozilla/5.0	no-cache	no-cache		text/x	ml,application	on/xml,app	x-gzip,	x-defla	ate, gzip, def	la utf-8, utf-8	en :	localhost:8	JSESSION
Normal	POST	Mozilla/5.0	no-cache	no-cache		text/x	ml,application	on/xml,app	x-gzip,	x-defla	ate, gzip, def	la utf-8, utf-8	en :	localhost:8	JSESSION
Normal	GET	Mozilla/5.0	no-cache	no-cache		text/x	ml,application	on/xml,app	x-gzip,	x-defla	ate, gzip, def	la utf-8, utf-8	en :	localhost:8	JSESSION
M	N		0	Р	C	2	R	S	1		U	V	W	X	Y
connection	lenght	content		classificati	URL										
close				0	http://	locall	nost:8080/tie	enda1/inde	ex.jsp H	HTTP/1	.1				
close				0	http://	locall	nost:8080/ti	enda1/pub	lico/an	adir.js	p?id=3&no	mbre=Vino-	Rioja⪯	cio=100&ca	antidad=55
Connection	Content-L	eid=3&no	mbre=Vino+Rio	ē 0	http://	locall	nost:8080/tie	enda1/pub	lico/an	adir.js	p HTTP/1.1				
close				0	http://	locall	nost:8080/tie	enda1/pub	lico/au	tentica	ar.jsp?modo	=entrar&log	gin=choong	g&pwd=d1s	e3ci%F3n
Connection	Content-L	modo=er	ntrar&login=cho	0	http://	locall	nost:8080/ti	enda1/pub	lico/au	tentica	ar.jsp HTTP	/1.1			
close				0	http://	locall	nost:8080/tie	enda1/pub	lico/ca	racteri	sticas.jsp?i	d=2 HTTP/1	.1		
Connection	Content-L	eid=2		0	http://	locall	nost:8080/ti	enda1/pub	lico/ca	racteri	sticas.jsp H	TTP/1.1			
close				0	http://	locall	nost:8080/ti	enda1/pub	lico/ca	rrito.js	p HTTP/1.1				
close				0	http://	locall	nost:8080/ti	enda1/pub	lico/en	trar.jsp	?errorMsg	=Credencia	les+incorre	ctas HTTP/	1.1

3. XSS Dataset has 13000 entry with Parameter Sentence and Label. Here Sentence denotes various string input specially html tags and Label works as XSS payload detector.

В	С	D
Sentence	Label	
0 <li><a class="image" href="/wiki/File:Socrates.png"><im< td=""><td>0</td><td></td></im<></a></li>	0	
1 <tt onmouseover="alert(1)">test</tt>	1	
2 <del>[   �����   ����   ��    ��</del>	0	
3 <del>[                                      </del>	0	
4 <sup>*</sup>	0	
5 < li id="cite_note-118"> <span class="mw-cite-backlink"></span>	0	
6 <li><a href="/wiki/Contextualism" title="Contextualism">0</a></li>	0	
7 < li id="cite_note-Representing_causation-95"> < span cla	. 0	
8 <a href="mailto:ref"><a href"=""><a href="mailto:ref"><a href"="">mailto:ref"&gt;<a href"="">mailto:ref</a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>	0	
9 + + + + + + + + + + + + + + + + + + +	0	

4. <a href="https://github.com/fmereani/Cross-Site-Scripting-XSS">https://github.com/fmereani/Cross-Site-Scripting-XSS</a> this link has three dataset named Payload.csv, XSSTesting.csv and XSSTrainning.csv. In payload.csv 2 parameter found like below

Payloads
http://www.nwce.gov.uk/search\_process.php?keyword=%22%3e%3cscript%3ealert Malicious
http://www.manchester.gov.uk/site/scripts/google\_results.php?q=%22%3e%253cscr Malicious
http://www.ldsmissions.com/us/index.php?action=missionary.info%3cmarquee%3ep Malicious
http://education.powys.gov.uk/english/adult\_ed/register.php?lforenam=\%22%3e%3c Malicious
http://www.northwarks.gov.uk/site/scripts/google\_results.php?q=%22%3e%253cscri Malicious
http://www.chaoticwars.co.uk/register.php?ref='%3e%3ciframe%20src=http://google Malicious

and Others has same parameters which is used 0 and 1 to detect various special character and input in URL and then detect the url is Malicious or Bening

Contains ScripTag Readable Contains Con

A	AY	AZ	ВА	ВВ	ВС	BD	BE	BF	BG	ВН	ВІ	BJ	BK	BL	BM	BN
าร	Contains (	Contains	ti Contains	Contains (	Contains C	Contains I	Contains I	Contains \	Contains F	Contains E	Contains A	Contains E	Letters Ra	Numbuers	Symbols F	Class
(	0	(	)	) 1	1 0	C	) 1	C	0	0	1	0	0.7614	0.0114	0.2273	Malicious
(	0	(	)	) 1	1 0	C	1	0	0	0	1	0	0.7614	0.0114	0.2273	Malicious
(	0	(	)	) 1	1 0	C	) 1	0	0	0	1	0	0.7203	0.0593	0.2203	Malicious
(	0	(	)	) (	0	C	1	C	0	0	1	0	0.7071	0.1065	0.1864	Malicious
(	0	(	)	) (	0	C	) 1	0	0	0	1	0	0.7158	0.1053	0.1789	Malicious
(	0	(	)	0	0	C	) 1	C	0	0	0	0	0.6483	0.1517	0.2	Malicious

5. <a href="https://github.com/fawaz2015/XSS-dataset">https://github.com/fawaz2015/XSS-dataset</a> another url analyzer type dataset which has 167 parameters to understand input URL

```
'url special characters',
                                          'html attr background',
       'url_tag_script',
                                              'html_attr_cite',
                                              'html_attr_classid'
       'url_tag_iframe',
                                              'html_attr_codebase',
       'url_tag_meta',
                                              'html_attr_data',
       'url_tag_applet
       'url_tag_object',
                                              'html attr dsync'
       'url_tag_embed',
                                              'html_attr_formaction',
       'url tag link',
                                              'html attr_href',
       'url_tag_svg',
                                              'html_attr_icon'
       'url_tag_frame',
                                              'html attr longdesc',
       'url_tag_form',
                                              'js_dom_windows',
                                              'is_dom_location',
       'url_tag_div',
                                              'js_dom_document',
       'url_tag_style'
                                              'js_prop_cookie',
       'url_tag_video',
       'url_tag_img',
                                              'js_prop_document',
       'url tag input',
                                              'js_prop_referrer',
       'url_tag_textarea',
                                              'js_method_write',
       'url_attr_action',
                                              'js_method_getElementById',
                                              'js_method_alert',
       'url attr_archive',
       'url_attr_background',
                                              'is method eval',
       'url_attr_classid',
                                              'is method fromCharCode',
                                              'js method prompt',
```

	BG	ВН	BI	BJ	BK	BL	BM	BN	ВО	BP	BQ
d js	method js	_method	js_method_j	s_method i	s min len	js_min_defj	s_min_fun	js_string_n	html_lengtl	Label	
1	0	0	0	0	11	0	1	353	11380	0	
1	0	0	0	0	267	0	0	4422	56223	0	
0	1	0	0	1	13	0	1	275	10712	1	
0	0	0	0	0	43	0	0	346	11922	0	
0	8	0	0	0	1879	2	15	1879	14735	1	
0	0	0	0	0	173	1	3	173	12324	0	
2	0	0	0	0	14	0	1	334	28684	0	
0	0	0	1	0	30	0	0	7533	151436	0	
0	1	0	0	0	10	0	0	139	15286	1	
2	0	0	0	0	82	0	2	2516	35728	0	
2	0	0	0	0		0	2			0	