# Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

# HTML Injection – Bypass Filters

# Filters / Escape HTML

```
>>>
>>> import cgi
>>>
>>>
>>> email = "<h1>Vulnerable to HTMLi</h1>"
>>>
>>> cgi.escape(email)
'&lt;h1&gt;Vulnerable to HTMLi&lt;/h1&gt;'
>>>
>>> email = " ' "
>>>
>>> cgi.escape(email)
" ' "
>>>
>>> email = """ " """
>>> cgi.escape(email)
' " '
>>>
```

# Why this confusion?

» Issue9061

classification

| | | | |
|---|---|---|---|
| **Title:** | cgi.escape Can Lead To XSS Vulnerabilities | | |
| **Type:** | security | Stage: | |
| Components: | Documentation, Library (Lib) | Versions: | Python 3.3, Python 3.2, Python 3.1, Python 2.7 |

process

| | | | |
|---|---|---|---|
| Status: | closed | Resolution: | duplicate |
| Dependencies: | | Superseder: | Copy cgi.escape() to html<br>View: 2830 |
| Assigned To: | docs@python | Nosy List: | Craig.Younkins, barry, docs@python, eric.araujo, fdrake, georg.brandl, orsenthil |
| Priority: | critical | Keywords: | |

Created on **2010-06-23 15:46** by **Craig.Younkins**, last changed **2010-08-24 01:31** by **benjamin.peterson**. This issue is now **closed**.

**Messages (10)**

**msg108457 - (view)** **Author: Craig Younkins (Craig.Younkins)** **Date: 2010-06-23 15:46**

```
The method in question: http://docs.python.org/library/cgi.html#cgi.escape
http://svn.python.org/view/python/tags/r265/Lib/cgi.py?view=markup   # at the bottom
http://code.python.org/hg/trunk/file/3be6ff1eebac/Lib/cgi.py#l1031

"Convert the characters '&', '<' and '>' in string s to HTML-safe sequences. Use this if you need to display text that might contain such characters in
HTML. If the optional flag quote is true, the quotation mark character ('"') is also translated; this helps for inclusion in an HTML attribute value, as
in <A HREF="...">. If the value to be quoted might include single- or double-quote characters, or both, consider using the quoteattr() function in the
xml.sax.saxutils module instead."

cgi.escape never escapes single quote characters, which can easily lead to a Cross-Site Scripting (XSS) vulnerability. This seems to be known by many,
but a quick search reveals many are using cgi.escape for HTML attribute escaping.
```

http://bugs.python.org/issue9061

# Can it do more?

## Escaping HTML

The `cgi` module that comes with Python has an `escape()` function:

Toggle line numbers

```
1 import cgi
2
3 s = cgi.escape( """& < >""" )   # s = "&amp;amp; &amp;lt; &amp;gt;"
```

However, it doesn't escape characters beyond `&`, `<`, and `>`. If it is used as `cgi.escape(string_to_escape, quote=True)`, it also escapes `"`.

https://wiki.python.org/moin/EscapingHtml

# Filter Code in Application

```
class HtmlInjection1Secure(webapp2.RequestHandler):
    def get(self):

        email = cgi.escape(self.request.get("email"))
```

# Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

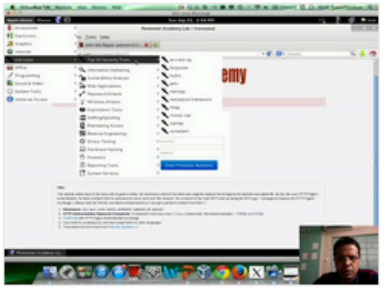

## Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

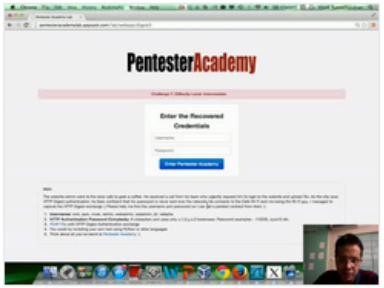
Start Learning Today!

## Latest Videos

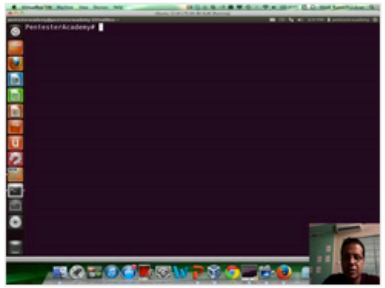
New content added weekly!



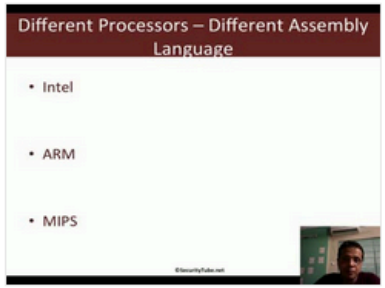
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges




Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux




Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux