

# A new form of general HTTP Layer 7 attack is now taking shape....

- Affects both Apache and IIS.
- Better evasion against DDOS protection systems.
- Enjoys a low attack nodes-to-target server ratio.

- Uses HTTP POST requests, instead of HTTP GET.
- “A POST request includes a message body in addition to a URL used to specify information for the action being performed. This body can use any encoding, but when webpages send POST requests from an HTML form element the Internet media type is "application/x-www-form-urlencoded". (source: Wikipedia - “POST (HTTP)”)”
- The field “Content-Length” in the HTTP Header tells the web server how large the message body is.

- The HTTP Header portion is complete and sent in full to the web server.
- Content-Length = 1000 bytes (for e.g.)
- The HTTP message body is properly URL-encoded, but .....

**.....is sent at, again for e.g., 1 byte per 110 seconds.**

- Multiply such connections by 60,000 and your web server will be DOS.



- Being “kind” folks, web servers will “obey” the “Content-Length” field to wait for the remaining message body to be sent.
- By waiting for the complete message body to be sent, web servers can support users with slow or intermittent connections.
- Most web servers can accept up to 2GB worth of content in a single HTTP POST request.



- Hence, any website which has forms, i.e. accepts HTTP POST requests, is susceptible to such attacks.
- Common uses of HTTP POST requests include logging in, uploading photo/video, sending webmail, attaching files in webmail, submitting feedback, updating account details and .....

# Why is This Attack Dangerous



- This attack can evade Layer 4 detection techniques as there is no malformed TCP, just like Slowloris.
- Unlike Slowloris, there is no delay in sending HTTP Header, hence nullifying IIS built-in defense, making IIS vulnerable too.
- Size, character sets and time intervals can be randomised to foil any recognition of Layer 7 traffic patterns by DDOS protection systems.

# Why is This Attack Dangerous

- All web sites with forms are vulnerable.  
(FFT: Which web sites do not have forms?)
- Difficult to differentiate from legit connections which are slow.
- **You only need up to 3 normal PCs (~60,000 connections) to DOS a web server, aka a “nuclear grade weapon” !!!**



## **Wong Onn Chee**

**Mobile: +65-98387930**

**onnchee@resolvo.com**



**Thank You**  
**for**  
**Your Attention**