Web Application Pentesting

Vivek Ramachandran

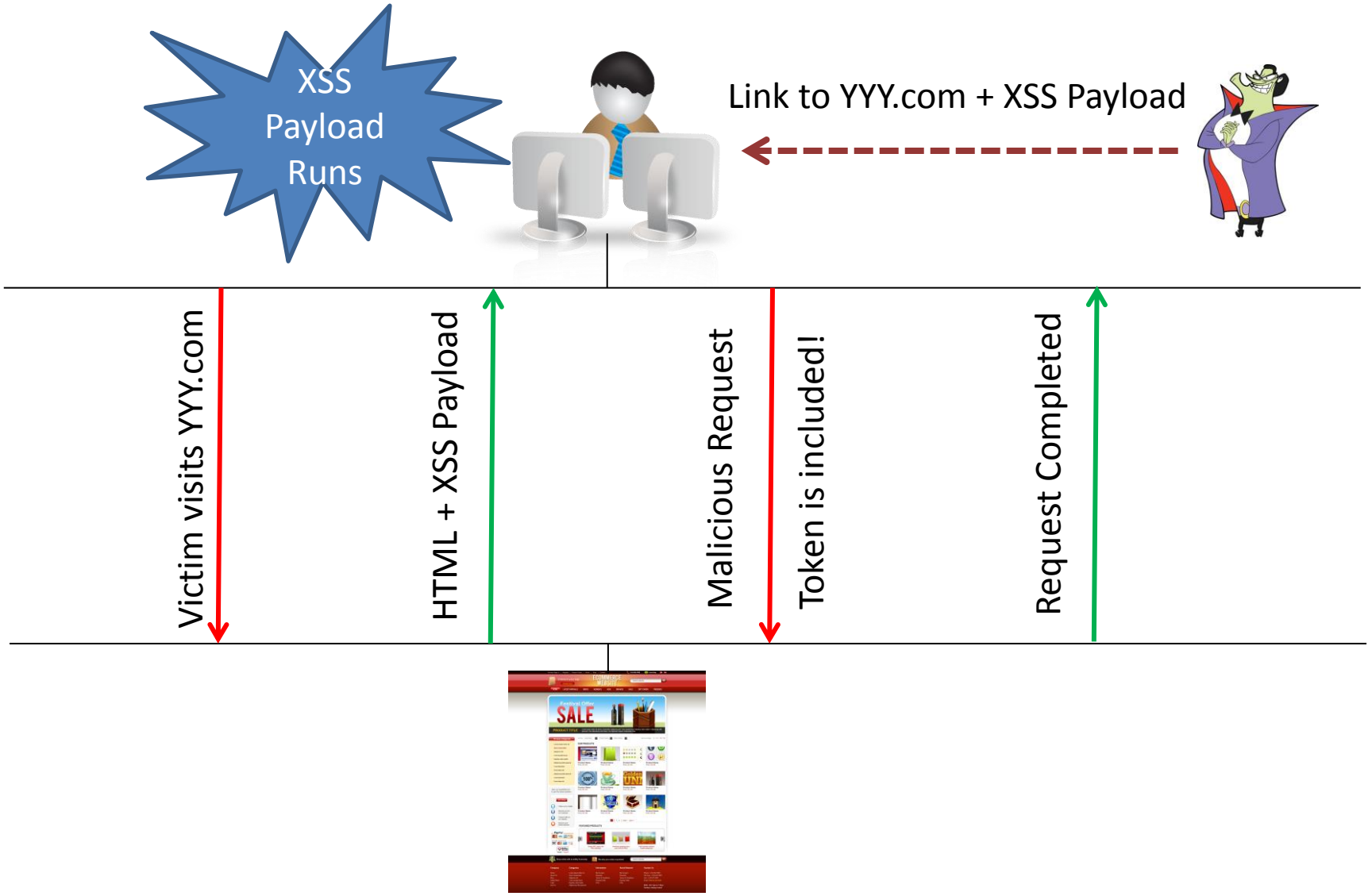
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

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

CSRF Token Bypass with XSS + Hidden Iframes

What if there is an XSS on the site?



Does the User Really have to visit the Real Website?

- Very noisy! User could suspect something!
- Easy to lure user to Attacker controlled website
- Can we leverage the discovered XSS there?

iframe

- An iframe is used to display a web page within a web page.
  - http://www.w3schools.com/html/html_iframe.asp
  - All origin policies apply within the frame

- Hidden iframe? ☺
  - Hide the frame from view entirely!

What the Attacker CAN/CANNOT do

- CAN:
  - Use XSS to run Payloads
  - Payload can post to Attacker's website
- CANNOT:
  - Read data directly from the embedded iframe
  - Not required in most cases

Pentester Academy