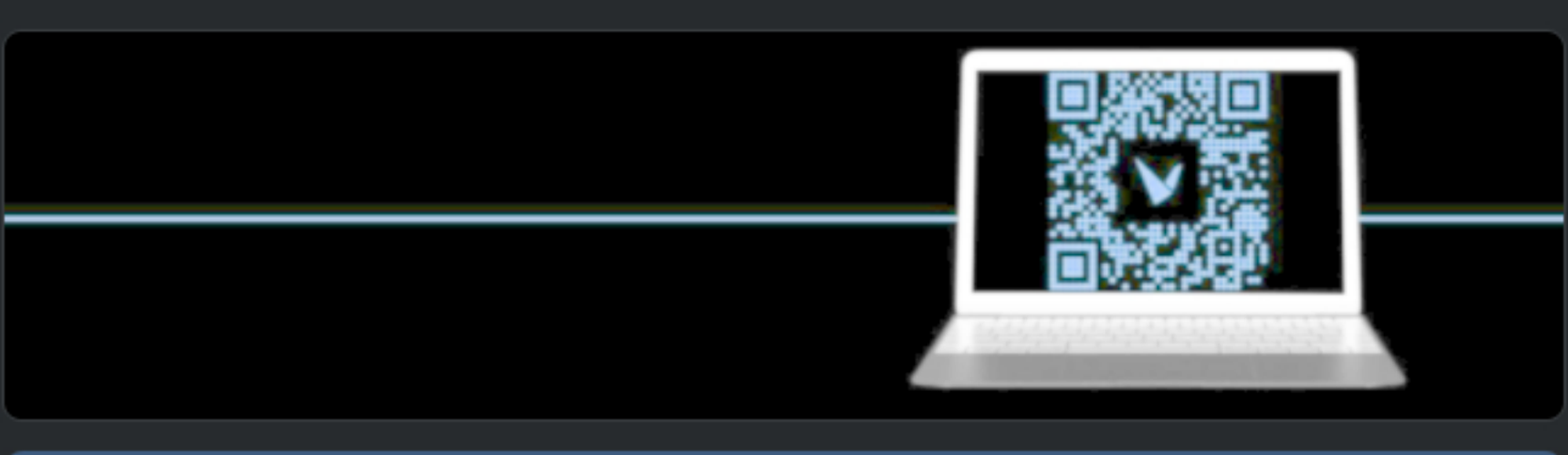

Week 2 Assignment Submission Form - Team 4

atharvajagdale45@gmail.com Switch account — Draft saved

* Required

Technical Assessment

KYC - Know Your Content for the week. This week's topic - **Clickjacking & HTML Injection** !

All the Best !

Which of the following should X-Frame-Options should be set to *

- [ ] DENY
- [ ] SAMEORIGIN
- [x] All of the above
- [ ] None of the above

What payload did you use for the lab "Let me Store them!" *

- [x] ">abc
- [ ] abc
- [ ] <abc></b/
- [ ] <abc></h1>

The correct sequence of HTML tags for starting a webpage is *

- [ ] HTML, Head, Body, Title,
- [x] HTML, Head, Title, Body
- [ ] HTML, Body, Title, Head
- [ ] Head, Title, HTML, body

The "ALLOW-FROM" URI means *

- [x] Permit the specified "uri" to frame this page
- [ ] Allow from anyone except the URI mentioned
- [ ] Allow only images from the URI
- [ ] Allow only text from the URI

______ defines that this document is an HTML5 document *

- [ ] <html>
- [x] <!DOCTYPE html>
- [ ] <!DOCUMENT html>
- [ ] <!DOCUMENT html5>

The severity of HTML Injection is *

- [ ] P5
- [x] P4
- [ ] P3
- [ ] P2

What website you would use in order to check if the website has the necessary headers or not *

- [ ] https://google.com
- [ ] https://securityheaders.com
- [ ] https://bing.com
- [x] All of the above

The impact of Click Jacking is *

- [ ] To gain followers on social media
- [ ] To gain RSS subscribers
- [ ] To transfer funds unknowingly from a victim
- [x] All of the above

If you find an HTML Injection there is a good chance of finding *

- [x] XSS
- [ ] XXE
- [ ] CSRF
- [ ] MFLAC

What payload did you use for the lab "HTML's are easy!" *

- [ ] "><h1>Hello World</h1>
- [x] <h1>Hello World</h1>
- [ ] "><h1>Hello World</h1>"<
- [ ] None of the above

ClickJacking on Logout and Contact form is sensitive *

- [ ] TRUE
- [ ] FALSE
- [ ] Maybe
- [x] Cant Say

The recommended clickjacking protection is to incorporate the frame-ancestors in CSP. The value of frame-ancestors should be set to *

- [ ] none
- [ ] self
- [ ] allow
- [x] Both A and B

The severity of ClickJacking on sensitive pages is *

- [ ] P5
- [ ] P3
- [x] P4
- [ ] P2

The CVSS score of HTML Injection is *

- [x] 0.1 - 3.9
- [ ] 4.0 - 6.9
- [ ] 7.0 - 8.9
- [ ] 9.0 - 10.0

The Clickjacking vulnerability we saw in "Let's Re-Hijack!" was to _____ *

- [x] Login into Google Account
- [ ] Delete User Account
- [ ] Delete Admin account
- [ ] All of the above

What payload did you use for the lab "File Names are also vulnerable!" *

- [ ] "><iframe src="malware_iframe.html">.txt
- [x] <iframe src="malware_iframe.html">.txt
- [ ] "><iframe src="malware_iframe.html".txt
- [ ] "><iframe><iframe src="malware_iframe.html">.txt

HTML Injection is exploited with? *

- [ ] Open Source Intelligence
- [x] Social Engineering
- [ ] Remote Code Execution
- [ ] None of the Above

ClickJacking on non-sensitive pages comes under which category? *

- [x] P5
- [ ] P4
- [ ] P3
- [ ] P2

What payload did you use for the lab "Encode IT!" *

- [ ] ROT encode of the payload <h1>Hello World</h1>
- [ ] Base64 encode of the payload <h1>Hello World</h1>
- [x] URL encode of the payload <h1>Hello World</h1>
- [ ] <h1>Hello World</h1>

Which of the following should be checked to know if page is vulnerable to clickjacking? *

- [ ] Content Security Policy
- [x] X-Content-Type-Options HTTP Header
- [ ] X-Frame-Options HTTP Header
- [ ] X-Powered-By

HTML stands for ? *

- [x] HyperText Markup Language
- [ ] HyperText and links Markup Language
- [ ] HighText Machine Language
- [ ] None of the above

Can Click Jacking be used to download a malware? *

- [x] True
- [ ] False

What payload did you use for the lab "File Content and HTML Injection a perfect pair!" *

- [x] A HTML file
- [ ] An SVG file with HTML tags
- [ ] A CSS file
- [ ] All of the above

HTML Injection can be prevented by *

- [ ] Checking if input contains tags or not
- [ ] Sanitizing the input
- [ ] Never trust user input
- [x] All of the above

Which of the following is used to prevent Clickjacking? *

- [ ] HTTPS Connection
- [ ] X-Frame-Options HTTP Header
- [x] Content-Security-Policy HTTP Header
- [ ] None of the above

ClickJacking is also known as ? *

- [x] User Interface redress attack
- [ ] UI redressing
- [ ] Both A and B
- [ ] None of the above

The Clickjacking vulnerability we saw in "Let's Hijack!" was to _____ *

- [ ] Delete User Account
- [ ] Login into Google Account
- [x] Delete Admin account
- [ ] Both A and C

Which of the following might be an injection point for HTML Injection *

- [ ] ?profileId=
- [ ] ?search=
- [ ] ?account=
- [x] ?redirect=

What payload did you use for the lab "Injecting HTML using URL" *

- [ ] <h1>Hello</h1> in the URL
- [x] ?<h1>Hello</h1> in the URL
- [ ] !<h1>Hello</h1> in the URL
- [ ] None of the above

The impact of HTML Injection is *

- [ ] Phishing
- [ ] Social Engineering
- [ ] Stealing Credentials
- [x] All of the above

A copy of your responses will be emailed to the address you provided.

Back | Submit | Page 4 of 4 | Clear form