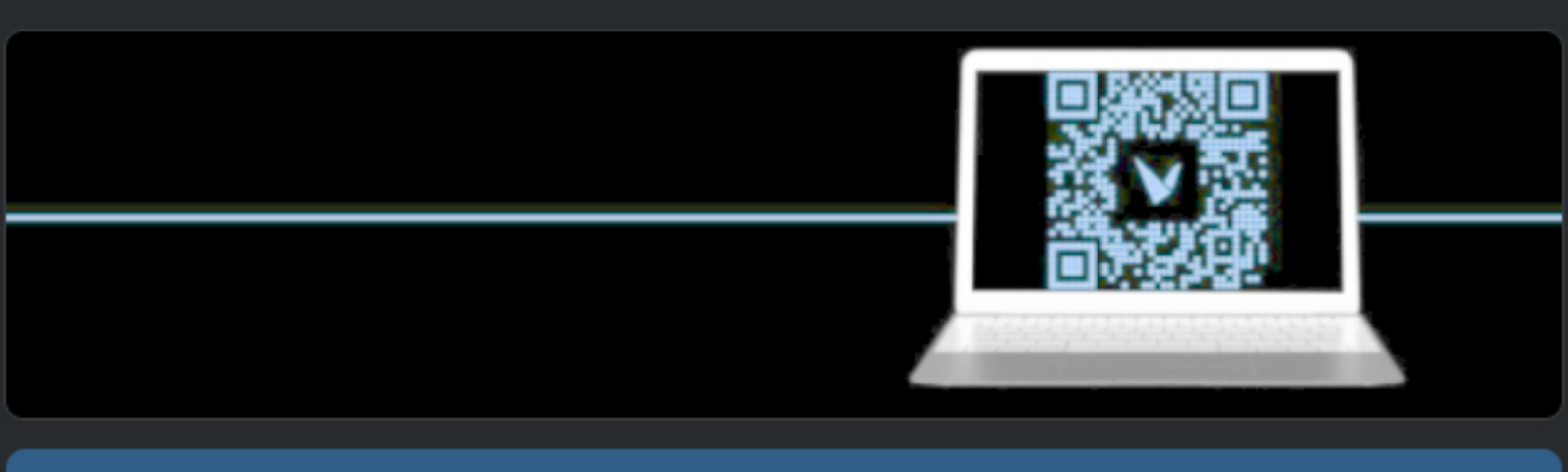

Week 5 - Assignment Submission Form

atharvajagdale45@gmail.com Switch account Draft saved

Week 5 Assessment

KYC - Know Your Content for the week. This week's topic - **Cross Origin Resource Sharing (CORS)** !

All the Best !

In the lab "CORS with Arbitrary Subdomain" the value of Origin header used was — 1 point

- ( ) hacktify.com
- ( ) hacktify.in
- ( ) somesubdomain.hacktify
- (x) somesubdomain.hacktify.in

Clear selection

CORS comes under which category — 1 point

- ( ) Broken Access Control
- ( ) Broken Authentication
- (x) Security Misconfiguration
- ( ) Insufficient Logging and Monitoring

Clear selection

What do you mean by "Access-control-allow-origin:attacker.com" — 1 point

- ( ) The vulnerable website will share its resources with everyone else except attacker.com
- (x) The vulnerable website will share its resources with attacker.com
- ( ) The vulnerable website will block attacker.com
- ( ) None of the above

Clear selection

If a user does not know to use curl he/she can use _____ instead — 1 point

- ( ) gau
- (x) waybackurls
- ( ) grep
- ( ) Burp Suite

Clear selection

In the lab "CORS with suffix match" the value of Origin header used was — 1 point

- ( ) hacktify.com
- ( ) evil.com
- ( ) evil.in
- (x) evilhacktify.in

Clear selection

In the command "curl example.com -I -H Origin: attacker.com" -H is used to — 1 point

- ( ) Show response with indentation
- (x) Send a custom header
- ( ) Return headers of the responses
- ( ) Tell curl that CORS is being performed

Clear selection

What is the severity of CORS where PII is leaked — 1 point

- ( ) P2
- (x) P3
- ( ) P4
- ( ) P5

Clear selection

Which one of the following is a prevention of CORS — 1 point

- ( ) Only allow trusted websites
- ( ) Proper configuration of cross-domain requests
- ( ) Remove Origin Header
- (x) Both A and B

Clear selection

Which one of the following is the curl command to check if example.com is vulnerable to CORS or not — 1 point

- ( ) curl example.com -H Origin: attacker.com
- ( ) curl example.com -I -H Origin: attacker.com
- (x) Both A and B
- ( ) None of the above

Clear selection

_____ should be avoided in internal networks — 1 point

- ( ) Blacklisting
- ( ) Wildcards
- (x) Both A and B
- ( ) None of the above

Clear selection

For which of the following case/s CORS CANNOT be exploited — 1 point

- ( ) Access-Control-Allow-Origin : website.com
- ( ) Access-Control-Allow-Origin : *
- (x) Access-Control-Allow-Origin : null
- ( ) All of the above

Clear selection

Avoiding whitelisting of _____ to prevent CORS — 1 point

- ( ) null
- ( ) #
- (x) Origin Header
- ( ) None of the above

Clear selection

In the CORS exploit script "this.readyState == 4" means — 1 point

- (x) Response is ready to be shown
- ( ) Request not initialized
- ( ) Server connection established
- ( ) Request is processing

Clear selection

What do you mean by "Access-control-allow-origin:*" — 1 point

- ( ) The vulnerable website will share its resources with everyone else except attacker.com
- ( ) The vulnerable website will share its resources with everyone
- ( ) The vulnerable website will share its resources with no one
- (x) None of the above

Clear selection

What was the payload used in the lab "CORS With Arbitrary Origin" — 1 point

- ( ) Add Original Header with value evil.com
- ( ) Add X-Frames-Origin Header with value evil.com
- (x) Add Origin Header with value evil.com
- ( ) None of the above

Clear selection

In the lab "CORS with Null origin" the value of access-control-allow-origin was — 1 point

- (x) null
- ( ) evil.com
- ( ) null.evil.com
- ( ) null.com

Clear selection

What is the severity of CORS where PII is not leaked — 1 point

- (x) P3
- ( ) P4
- ( ) P5
- ( ) None of the above

Clear selection

In the command "curl example.com -I -H Origin: attacker.com" -I is used to — 1 point

- (x) Show response with indentation
- ( ) Send a custom header
- ( ) Return headers of the responses
- ( ) Tell curl that CORS is being performed

Clear selection

CORS extends and adds flexibility to — 1 point

- ( ) Same-Origin Policy
- (x) Cross-Origin Policy
- ( ) Content Security Policy
- ( ) None of the above

Clear selection

Which one of the following is not a test case of CORS — 1 point

- ( ) Access-control-allow-origin:attacker.com
- ( ) Access-control-allow-origin:*
- ( ) Access-control-allow-origin:null
- (x) Access-control-allow-origin:#

Clear selection

In the lab "CORS with Escape dot" the value of Origin header used was — 1 point

- ( ) hacktify.in
- (x) wwwhacktify.in
- ( ) www.hacktify.in
- ( ) www.in

Clear selection

Which one of the following is NOT an impact of CORS — 1 point

- ( ) Account Takeover
- ( ) Sensitive Data Exposure
- ( ) Cookie Stealing
- (x) Database exposure

Clear selection

CORS protocol uses ____ to trust web origins — 1 point

- ( ) Cookies
- ( ) HTTPS
- (x) HTTP Headers
- ( ) All of the above

Clear selection

The CORS exploit script is written in — 1 point

- (x) HTML
- ( ) AJAX
- ( ) JavaScript
- ( ) PHP

Clear selection

In the lab "CORS with Substring match" the value of Origin header used was — 1 point

- ( ) hacktify.com
- (x) hacktify.co
- ( ) co.hacktify.co
- ( ) hacktify.in

Clear selection

The first header which we should look out while exploiting CORS is — 1 point

- ( ) Access-Common-Allow-Origin
- (x) Access-Control-Allow-Origin
- ( ) Access-Common-Deny-Origin
- ( ) Access-Control-Deny-Origin

Clear selection

CORS Stands for — 1 point

- ( ) Cross Origin Resource Swapping
- (x) Cross Origin Resource Sharing
- ( ) Cross Operation Resource Sharing
- ( ) Cross Operation Resource Swapping

Clear selection

In the lab "CORS with prefix match" the value of Origin header used was — 1 point

- (x) hacktify.in.evil.com
- ( ) hacktify.evil.com
- ( ) hacktify.com
- ( ) evil.com

Clear selection

The second header which we should look out while exploiting CORS is — 1 point

- (x) Access-Control-Allow-Credentials
- ( ) Access-Common-Allow-Credentials
- ( ) Access-Control-Deny-Credentials
- ( ) Access-Common-Deny-Credentials

Clear selection

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

Back | Submit | Page 4 of 4 | Clear form