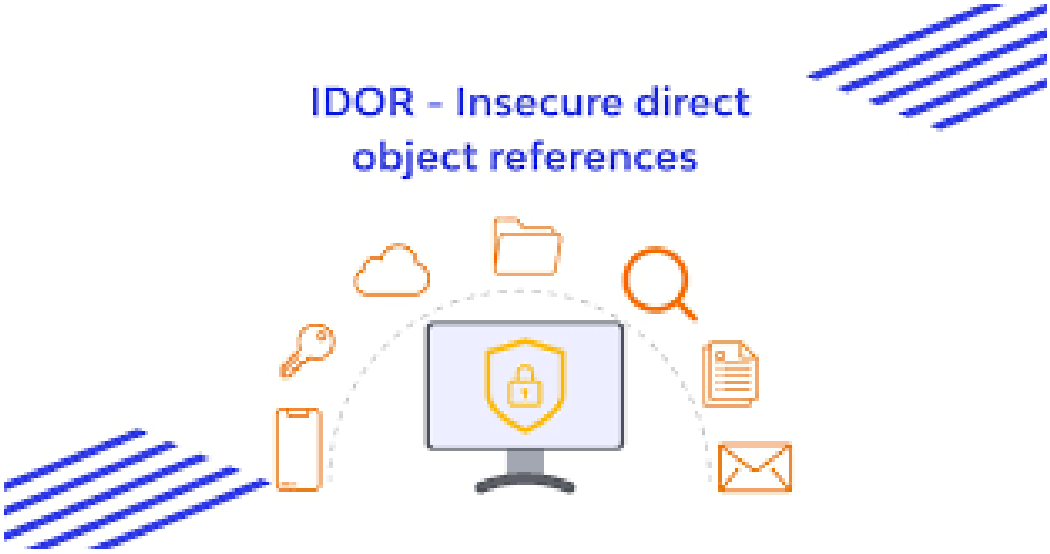
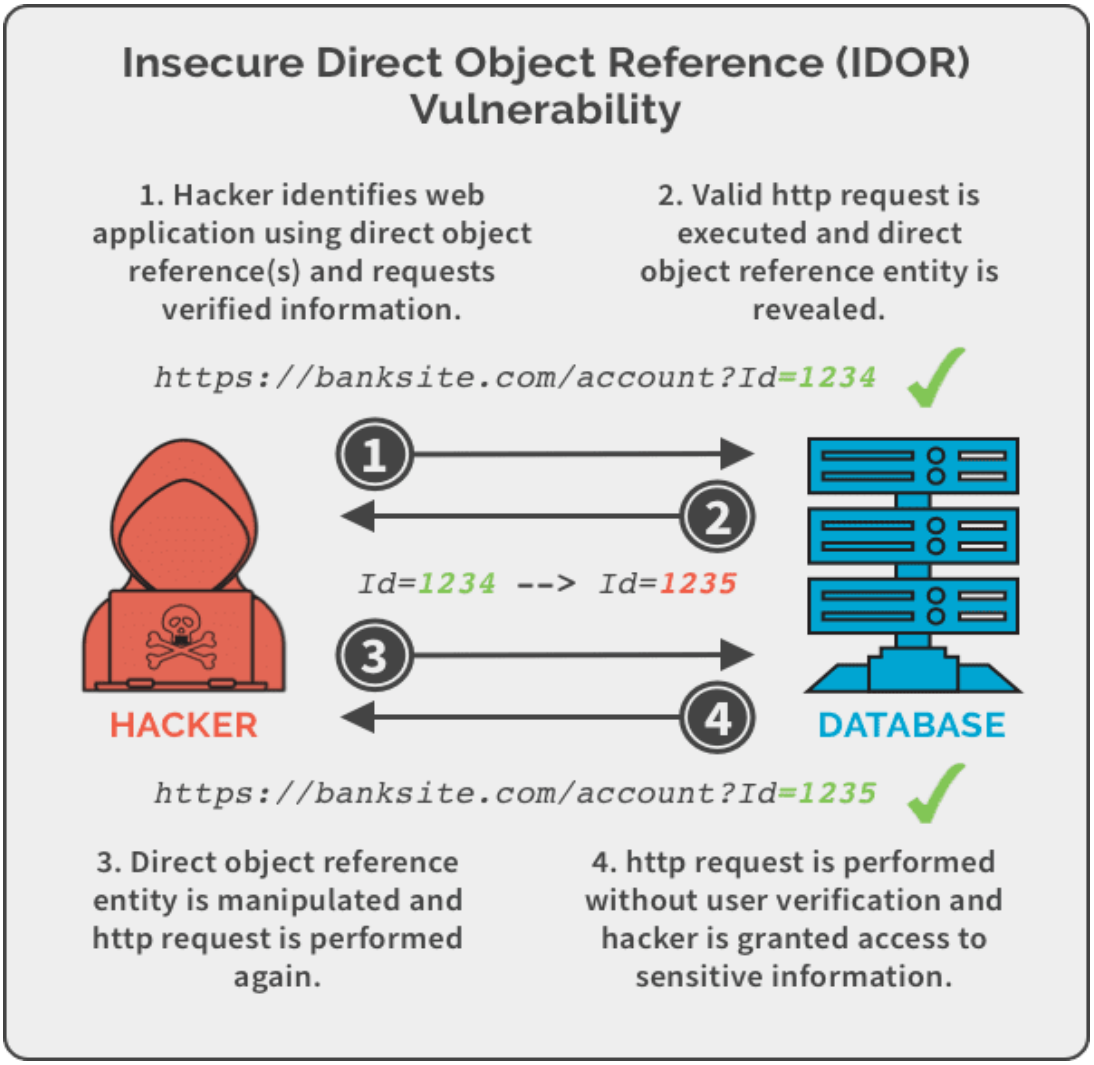
Insecure Direct Object Reference & HTTP Security Headers



Insecure Direct Object Reference (IDOR):

- IDOR stands for Insecure Direct Object Reference.
- It's a security vulnerability that occurs when an application allows users to access objects (like files, database records, or URLs) directly based on user-supplied input, such as input parameters or cookies.
- Attackers can manipulate these references to access unauthorized data or perform actions they're not supposed to.



Impact of IDOR:

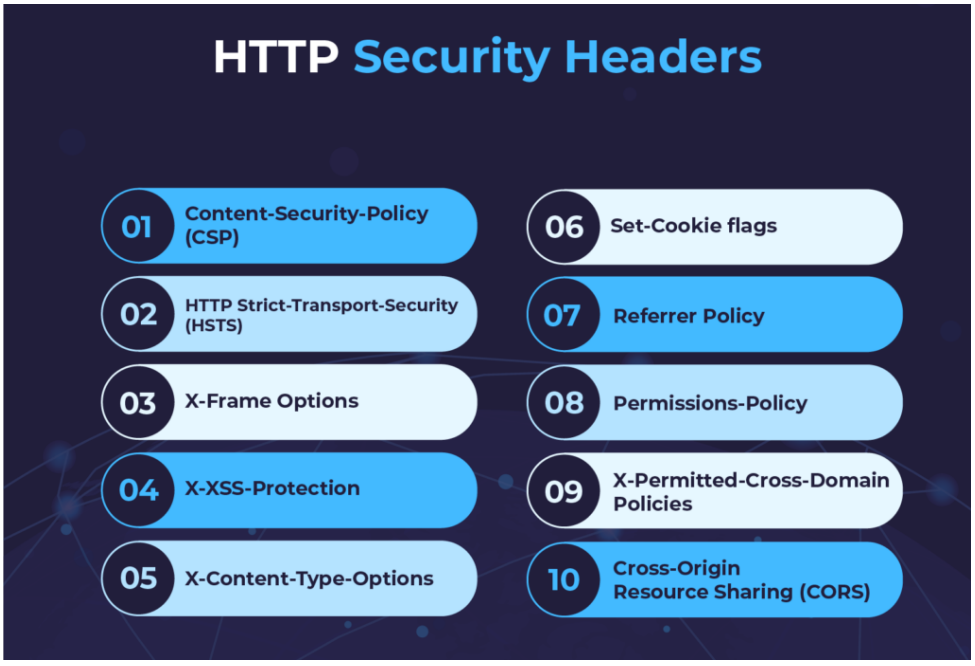
The impact of IDOR can be severe and includes:

- Unauthorized access to sensitive data.
- Data tampering, where attackers can modify data.
- Privilege escalation, allowing users to gain higher-level access.
- Exposure of personal information, financial data, or confidential records.
- Potential for data loss or corruption.

HTTP Security Headers:

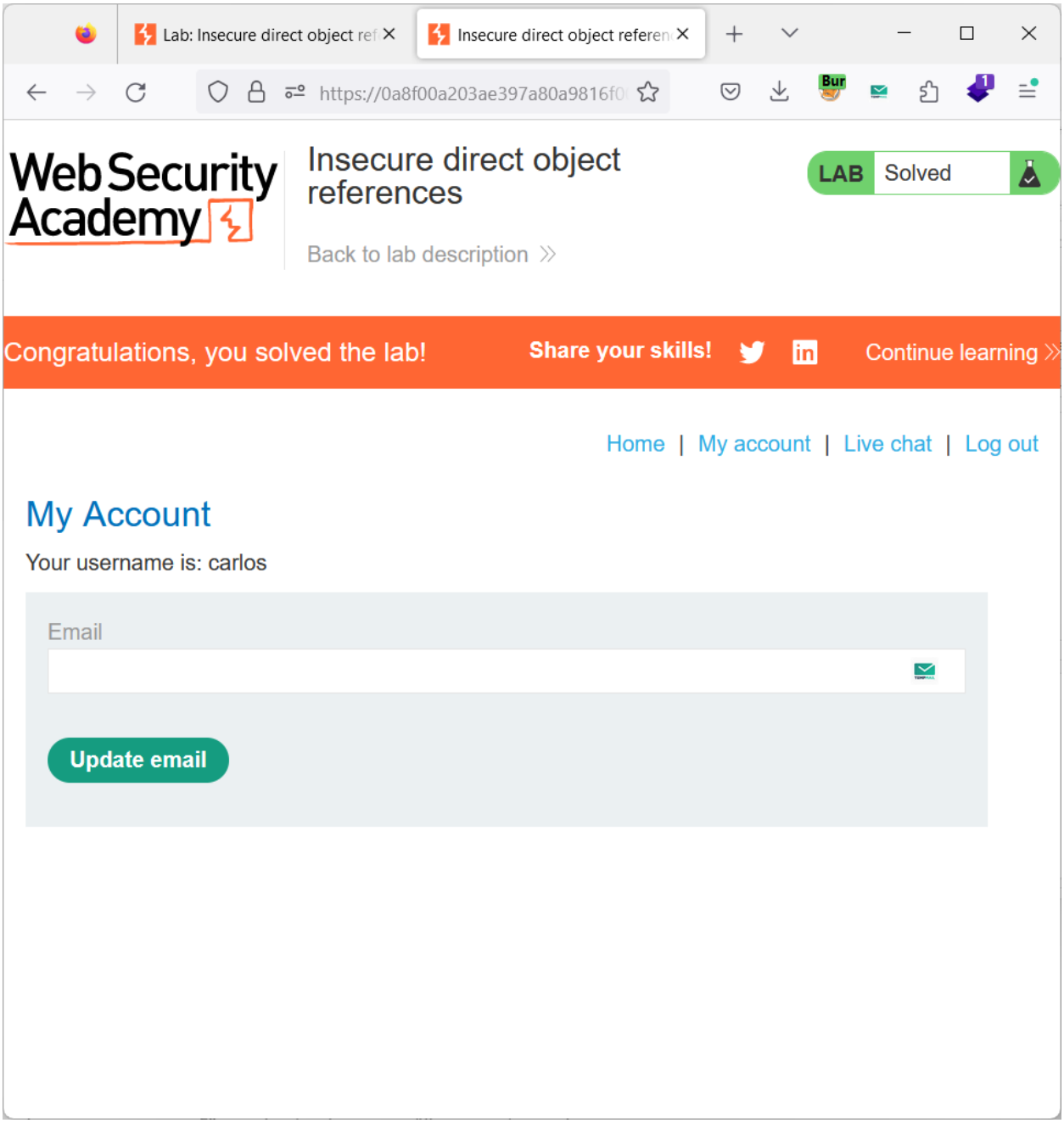
- HTTP Security Headers are response headers sent by a web server to instruct browsers on how to behave when interacting with a web page.
- They help enhance the security of web applications by mitigating various threats.

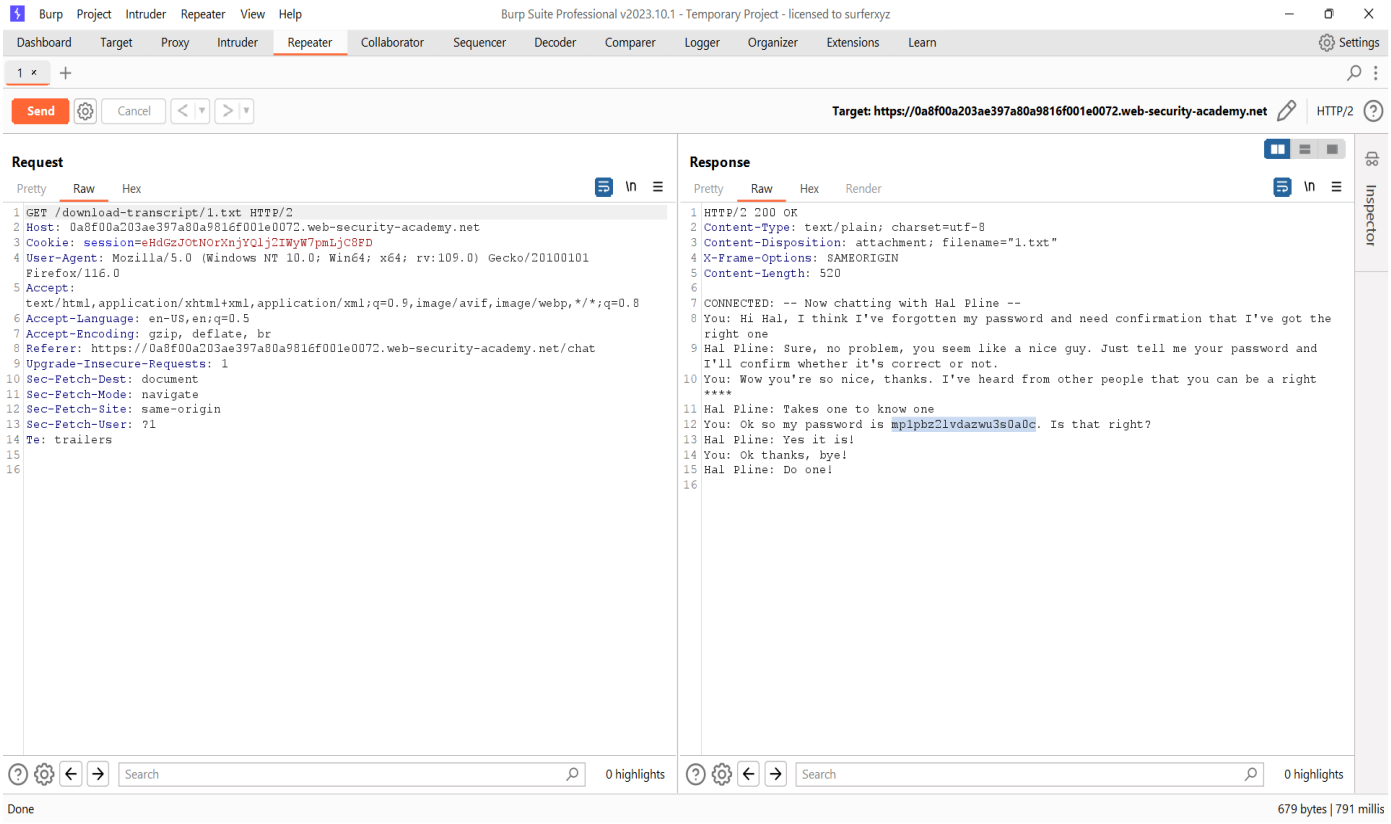
Different Types of Security Headers:



- Content-Security-Policy (CSP):
    - Specifies allowed content sources, preventing XSS and data injection.
- X-Content-Type-Options:
    - Prevents MIME type sniffing by browsers, enhancing data integrity.
- X-Frame-Options:
    - Controls iframe embedding to prevent clickjacking.
- X-XSS-Protection:
    - Enables XSS filters in browsers.
- Strict-Transport-Security (HSTS):
    - Enforces HTTPS usage to thwart MITM attacks.
- Referrer-Policy:
    - Controls HTTP Referrer header to enhance privacy.
- Feature-Policy:
    - Specifies which web features are allowed.
- Expect-CT:
    - Enforces Certificate Transparency for SSL/TLS certificates.
- Cross-Origin-Resource-Policy: -
    - Controls handling of cross-origin requests.
- Public-Key-Pins (HPKP) (deprecated):
    - Specified valid public keys for SSL/TLS certificates (no longer recommended).

Practical


Lab: Insecure direct object ref
Insecure direct object referen
https://0a8f00a203ae397a80a9816f0
Web Security Academy
Insecure direct object references
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Live chat | Log out
My Account
Your username is: carlos
Email
Update email


Burp Project Intruder Repeater View Help
Burp Suite Professional v2023.10.1 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 ×
Send Cancel
Target: https://0a8f00a203ae397a80a9816f001e0072.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
1 GET /download-transcript/1.txt HTTP/2
2 Host: 0a8f00a203ae397a80a9816f001e0072.web-security-academy.net
3 Cookie: session=eHdGzJOtNOrXnjYQlj2IWyW7pmLjC8FD
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a8f00a203ae397a80a9816f001e0072.web-security-academy.net/chat
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 520
6
7 CONNECTED: -- Now chatting with Hal Pline --
8 You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
9 Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
10 You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
11 Hal Pline: Takes one to know one
12 You: Ok so my password is mp1pbz2lvdazwu3s0a0c. Is that right?
13 Hal Pline: Yes it is!
14 You: Ok thanks, bye!
15 Hal Pline: Do one!
16
Search 0 highlights
Inspector
Done
679 bytes | 791 millis

References

1. https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference
2. https://portswigger.net/web-security/access-control/idor
3. https://www.invicti.com/blog/web-security/http-security-headers/
4. https://www.loginradius.com/blog/engineering/http-security-headers