✓ Choose the correct payload to exploit the lab Get The 127.0.0.1 * 1/1

- ○ localhost
- ○ www.google.com
- ◉ 127.0.0.1:80 ✓
- ○ None of the above

✓ Which of the following is payload would solve the lab http(s)? Nevermind!! * 1/1

- ○ 127.0.0.1:80
- ○ localhost
- ○ http://127.0.0.1:80
- ◉ http://localhost:80 ✓

✓ To solve the lab ":" The saviour! Choose a accurate payload from the given choices * 1/1

- ○ http://127.0.0.1:80
- ○ http://[::]:80/
- ○ http://localhost:80

- (selected) http:://[:]:80/ ✓

✓ Lab Messed Up Domain! can be solved using which of the following payloads? * 1/1

- ( ) www.google.com
- ( ) http://localhost:80
- (selected) http://customer1.app.localhost.my.company.127.0.0.1.nip.io/ ✓
- ( ) 127.0.0.1:80

✓ Choose a correct solution for lab Decimal IP? * 1/1

- (selected) http://213070643 ✓
- ( ) http://3232235521
- ( ) http://3232235777
- ( ) http://2852039166

✓ Which of the following is payload would help you to solve the lab Short-hand IP address * 1/1

- ( ) http://127.0.2
- ( ) http://0/

- [ ] http://127.1
- [x] Both C and D ✓

✓ The lab File Upload to SSRF! the SSRF attack was possible using the request catcher tools by using payloads in which of the following fields? * 1/1

- [ ] File Name
- [x] File Contents ✓
- [ ] Text Input Box
- [ ] Both A and C

✓ Choose the correct payload to exploit the lab SSRF with DNS Rebinding * 1/1

- [ ] localhost
- [x] b0x.mannulinux.org ✓
- [ ] www.google.com
- [ ] Both A and B

✓ Which payload would you use to get metadata from the lab SSRF on Cloud? * 1/1

- [ ] http://metadata.google.internal/computeMetadata/v1/
- [ ] localhost

- [ ] http://169.254.169.254/latest/meta-data/iam/security-credentials/
- [x] Both A and C ✓

✓ What does SSRF stands for _____ * 1/1

- [ ] Server Script Response Forgery
- [x] Server Side Request Forgery ✓
- [ ] Server Side Response Forgery
- [ ] Server Script Request Forgery

✓ Server Side Request Forgery is a web security vulnerability which allows attacker to induce _____ application to make _____ requests to an arbitrary domain controlled by an attacker. * 1/1

- [ ] Client-Side, FTP
- [x] Server-Side, FTP ✓
- [ ] Server-Side, HTTP
- [ ] Client-Side, HTTP

✓ Which of the following is the basic entity for testing a SSRF vulnerability onto a web application? * 1/1

- [ ] Request
- [x] Parameter ✓

Parameter ✓

- Response
- Header

✓ What do you mean by SSRF attacks against the server itself? * 1/1

- Attacker is able to access of victims account.
- (✓) Attacker makes a request to local machine to gain administrative rights
- Attacker is able to get access to public server
- Attacker is unable to access of victims account.

✓ Through a ssrf attack, the attacker might cause the server to make a connection to _____ services within the organization's infrastructure * 1/1

- (✓) Internal
- External
- Public
- None of the above

✓ Which of the following is the function of Burp Collaborator? * 1/1

- It provides DNS services
- It provides an HTTP/HTTPS service
- It provides an SMPT/SMTPS service

All of the above ✓

✓ A successful SSRF attack may also allow an attacker to perform _____ execution. * 1/1

- SQL queries
- Command ✓
- Response
- Both B and C

✓ Sometimes SSRF attacks can also lead to which of the following attacks? * 1/1

- Cross-Site Scripting
- SQL Injection
- Remote Code Execution ✓
- Cross Site Request Forgery

✓ Server-Side Request Forgery (SSRF) refers to an attack, wherein an attacker can send a crafted _____ from a _____ web application. * 1/1

- Request, Secured
- Request, Vulnerable ✓

Response, Secured

Response, Vulnerable

✓ What would be your first step to perform a successful SSRF attack onto a vulnerable web application * 1/1

- (●) Identify the parameter on a web application ✓
- ( ) Send the request to the intruder tab of Burp Suite
- ( ) Check if you received an connection into your Burp Collaborator
- ( ) None of the Above

✓ Can a SSRF attacks be possible even bt black listing based on input filters * 1/1

- ( ) TRUE
- (●) FALSE ✓
- ( ) Network Scandal
- ( ) Cross Domain Scandal

✓ Which of the following cannot be used as an alternative of Burp Collaborator? * 1/1

- ( ) Requestcatcher.com
- (●) Tinyurl.com ✓

- Requestbin.com
- Webhook.site

✓ To bypass White Listing based on Input filters which of the following special character should be used to embed credentials in a URL before the hostname ? * 1/1

- #
- (●) @ ✓
- *
- &

✓ SSRF is mainly used to target internal systems behind the _____, that are unreachable to an attacker from the external network. * 1/1

- (●) Web Application Firewall ✓
- Organization
- Hidden Layer
- Server

✓ In which of the following tab of burp suite you can check for connections received by the vulnerable web application server? * 1/1

- Sequencer
- Intruder

Intruder

Extender

Burp Collaborator ✓

✓ Which of the following is a prevention of SSRF attack? * 1/1

Disable all user inputs

Enable Authentication on all Services

Whitelist Domain in DNS

Both B and C ✓

✓ Which of the following can be gained by a attacker through a successful SSRF attack? * 1/1

Gather information about the ports

Fingerprinting intranet

Can gain administrative rights to access the server.

All of the above ✓

✓ It's also possible for an attacker to mark SSRF, for accessing services from the same server that is listening on the _____ interface address. 1/1

Loopback

Public IP address

- [ ] 127.0.0.1
- [x] Both A and C ✓

✓ By enforcing URL schemes to prevent SSRF attacks which of the following URL scheme is not needed to be blocked? 1/1

- [ ] ftp://
- [x] https:// ✓
- [ ] http://
- [ ] file://

✓ Burp Collaborator uses its own dedicated _____ , and the server is registered as the authoritative _____ server for this domain. * 1/1

- [x] Domain name, DNS ✓
- [ ] Server Name, Host
- [ ] Sender name, Public
- [ ] Device name, Host

✓ SSRF is tricky vulnerability that abuses the most trust component which is the _____. * 1/1

- [ ] CA Certificate
- [x] Application's Code ✓

- [ ] User Data
- [ ] None of the Above