✓ Which of the following parameter did you use to exploit lab Give me my account!! * 1/1

- ○ name=
- ○ uid=
- ◉ id= ✓
- ○ profile=

✓ What sensitive data of victim did gain by exploiting lab Give me my account!! * 1/1

- ○ password of user
- ○ credit card number
- ○ latest bank transactions
- ◉ Both B and C ✓

✓ Identify the vulnerable parameter for lab Stop polluting my Params! * 1/1

- ○ uid=
- ○ name=
- ○ profile

- [x] id=

✓ Which of the following sensitive data of user can be altered in lab Stop Polluting my Params! * 1/1

- [x] username
- [ ] credit card number
- [ ] password of user
- [ ] profile picture of user

✓ Which of the following parameter is vulnerable to IDOR attack in lab Someone Changed my Password ! * 1/1

- [ ] password=
- [ ] user=
- [x] username=
- [ ] id=

✓ Identify the field or the user input which lead you to account take over in lab Someone Changed my Password ! * 1/1

- [ ] New Password
- [ ] Confirm Password

Password

Both A and B ✓

✓ Which of the following is the default request method used in lab Change your methods! Which could be modified later? * 1/1

POST

PUT

GET ✓

None of the Above

✓ What does IDOR stand for ? * 1/1

Insure Direction Object Reference

Insecure Direct Object Reference ✓

Insecure Direct Object Response

Initialized Direct Object Response

✓ Which of the following is not a type of IDOR attack? * 1/1

URL Tampering

Tampering Server Configurations ✓

Body Manipulation

- [ ] Both A and C

✓ In which of the following categories of OWASP top 10 2017 does IDOR belongs to ? * 1/1

- [ ] Insecure Deserialization
- [ ] XML External Entities
- [x] Broken Access Control ✓
- [ ] Security Misconfigurations

✓ ____ is a web application design method in which entity names are used to identify application-controlled resources that are passed in URLs or request parameters. * 1/1

- [x] Direct Object Reference ✓
- [ ] Document Object Model
- [ ] Model View Architecture
- [ ] REST API

✓ An insecure direct object reference (IDOR) is an _____ type of vulnerability. * 1/1

- [ ] Service-Control
- [ ] Domain-Control

Request-Control

Access-Control ✓

✓ IDOR vulnerabilities occurs when _____ user input can be used to gain _____ to resources. * 1/1

- Invalidated, Unauthorized access ✓
- Validated, Authorized access
- Validated, Unauthorized access
- Invalidated, Authorized access

✓ From the given URL: https://myaccount.com/profile.php?profilenm=admin&file=text.pdf according to you which of the parameter would help you to hunt for IDOR vulnerability if the application is vulnerable. * 1/1

- file=
- profilenm= ✓
- Both A and B
- None of the above

✓ When an IDOR attacks generally occurs? * 1/1

- Direct access to the server configurations
- Direct execution of malicious code onto the server

Direct execution of malicious code onto the server

- [x] Direct access by using user-supplied input to an object with no authorization
- [ ] Both B and C

✓ To start hunting for IDOR vulnerabilities which of the following is a basic or the initial step? * 1/1

- [ ] Setup your Burp Collaborator
- [x] Find a vulnerable parameter
- [ ] Change the value of the parameter
- [ ] Analyze the received Response from the server

✓ An IDOR vulnerability lets an attacker to gain administrative access to the server? * 1/1

- [ ] TRUE
- [x] FALSE

✓ Insecure Direct Object Reference represents a vulnerable _____ Reference. * 1/1

- [x] Document Object
- [x] Direct Object
- [ ] Model Object
- [ ] None of the Above

✓ The severity of an IDOR vulnerability varies from _____ to _____ depending upon the user data being exposed. * 1/1

- ○ P3,P4
- ○ P3, P5
- ◉ P2, P3 ✓
- ○ P4, P5

✓ If attacker come across a parameter named username in the URL of vulnerable web application and he tries for some random usernames and he successfully gains access to the random username profile will it be termed as IDOR vulnerability? * 1/1

- ◉ YES ✓
- ○ NO

✓ Which of the following parameters would help an attacker to perform a successful IDOR attack? * 1/1

- ○ id=
- ○ username=
- ○ lang=

- [x] Both A and B ✓

✓ IDOR creates an conducive environment for attackers to steal and access _____ * 1/1

- [ ] Sensitive Server Configurations
- [ ] Authorized Data
- [ ] Freely Available Data
- [x] Unauthorized Data ✓

✓ Attackers can bypass the _____ mechanism to access resources in the system directly by exploiting IDOR vulnerability * 1/1

- [x] Authorization ✓
- [ ] Confidentiality
- [ ] Integrity
- [ ] None of the Above

✓ What does the IDOR vulnerability endangers? * 1/1

- [ ] Availability of Server
- [ ] Privacy of Server
- [x] Privacy of Users ✓

- [ ] All of the above

✓ Which of the following user data would a attacker be able to gain if the web application is vulnerable to IDOR? * 1/1

- [ ] User Posted Posts
- [ ] User Posted Videos
- [ ] Users Personal Details
- [x] All of the above ✓

✓ Every resource instance can be called as an object and often, represented with an unique _____ 1/1

- [ ] URL
- [x] ID ✓
- [ ] Request
- [ ] Device

✓ Which of the following would help to prevent IDOR vulnerability? 1/1

- [ ] Never use an Indirect Reference Map
- [ ] Use an Indirect Reference Map

- ○ Validate User access
- ◉ Both B and C ✓

✓ _____ backs up your online data and restores it in the event of a cyberattack incident, including a data breach due to IDOR vulnerability. * 1/1

- ○ Monitoring
- ◉ Snapping ✓
- ○ Hijacking
- ○ Sniffing

✓ To mitigate IDOR attacks tokens should be generated in such a way that it can only be mapped to the user and is not public. * 1/1

- ◉ TRUE ✓
- ○ FALSE

✓ Which of the following are the remediates to IDOR attacks? * 1/1

- ○ Validation of parameters
- ○ Ensure that queries are scoped to the owner of the resource.
- ○ Verification of all the referenced objects should be checked.
- ◉ All of the above ✓

This form was created inside of VT.

Forms