Assignment checklist &

documentation

BENR 3433 INFORMATION SECURITY

YOUR AZUREWEBSITES LINK HERE FOR PENETRATION TESTING

# ?Your VMS architecture? ?threat modelling?

?due diligence?

Public connections over the Internet



Attacker? Visitor? Host? or Security?



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat Agent** | **Attack surface** | **Attack Goal** | **Impact** | **Controls (Mitigation)** |
| User credential stored in the database?? | Attacker? Visitor? Host? or Security? | Improper API implementation of the backend server? | Obtained user credential? | Confidentiality? Integrity? Availability? | ? |
|  |  | A lot more? |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 1 | Public API for security to create new host account.   * 1. API required security approval (e.g. /create/host)   2. Testing API without security approval (e.g. /create/test/host) | ?POST? https://xxxx.azurewebsites.net/??? |
| 2 | Public API for authenticated host to see all created visitors. |  |
| 3 | Public API for authenticated host to issue visitor pass (only visitor record stored into database, no need to create visitor account). |  |
| 4 | Public API for visitor to retrieve the pass. |  |
| 5 | Administrator login page (dump all hosts’ data upon successful  login). |  |
| 6 | * 1. Additional APIs (manage account roles (security/host) by   authenticated administrator and etc)   * 1. Public API for authenticated security to retrieve the contact number of the host from the given visitor pass (the pass should only review destination host to visit to the public) |  |

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 1 | Public API for security to create new host account.   * 1. API required security approval (e.g. /create/host)   2. Testing API without security approval (e.g. /create/test/host) |  |
|  | * 1. ?POST? <https://xxxx.azurewebsites.net/>???   2. ?POST? <https://xxxx.azurewebsites.net/>??? |

and the documentation on how to create new host and new test host (without security approval) The test API should have identical role as actual host

*The test API shall be removed at the end of the penetration testing.*

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 2 | Public API for authenticated host to see all created visitors. | |

and the documentation on how to see all created visitors by the host.

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 3 | Public API for authenticated host to issue visitor pass (only visitor record stored into database, no need to create visitor account). | |

and the documentation on how to issue visitor pass.

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 4 | Public API for visitor to retrieve the pass. |  |

and the documentation on how to access the created pass.

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 5 | Administrator login page (dump all hosts’ data upon successful  login). | |

and the documentation on how to login

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 6 | * 1. Additional APIs (manage account roles (security/host) by authenticated administrator and etc)   2. Public API for authenticated security to retrieve the contact number of the host from the given visitor pass (the pass should only review destination host to visit to public) | |

and the documentation on how to use the 6.1 and 6.2 APIs

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 1 | Public API for security to create new host account.  1.1 API required security approval (e.g. /create/host) | ?POST? https://xxxx.azurewebsites.net/??? |
|  | Current weakness and plan to secure it. | Expected outcomes and estimated date of completion |

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 2 | Public API for authenticated host to see all created visitors. | |
|  | Current weakness and plan to secure it. | Expected outcomes and estimated date of completion |

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 3 | Public API for authenticated host to issue visitor pass (only visitor record stored into database, no need to create visitor account). | |
|  | Current weakness and plan to secure it. | Expected outcomes and estimated date of completion |

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 4 | Public API for visitor to retrieve the issued pass. |  |
|  | Current weakness and plan to secure it. | Expected outcomes and estimated date of completion |

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 5 | Administrator login page (dump all hosts’ data upon successful  login). | |
|  | Current weakness and plan to secure it. | Expected outcomes and estimated date of completion |

|  |  |  |
| --- | --- | --- |
|  | **Needed APIs for BENR3433** | **API hosted at azurewebsites** |
| 6 | * 1. Additional APIs (manage account roles (security/host) by authenticated administrator and etc)   2. Public API for authenticated security to retrieve the contact number of the host from the given visitor pass (the pass should only review destination host to visit to public) | |
|  | Current weakness and plan to secure it. | Expected outcomes and estimated date of completion |

# Due diligence in securing your MongoDB database

|  |  |  |
| --- | --- | --- |
|  | **Database access (action plan)** | **Outcomes** |
| 1 | Backend uses certificates rather than username and password to connect to the MongoDB Atlas? | |
| 2 | Whitelist only the azurewebsites’ backend IP address? | |
| 3 | MongoDB Atlas uses strong username and password to login? | |