Solution Document

Tutor-Marked Assessment 4

Required October 21st, 2018

BIT695 – Web Technologies

By Gareth Worboys (student number 3318840)

Task 1: Security and availability

1. Do you think the web application for the case study would be considered secure and pass any of the tests according to the OWASP? Comment on the security and the pass/fail state of the web application. Discuss at least three examples from the web application relating to security and/or issues identified by the OWASP to support your answer.

Accurate documentation is one of the first major initiatives of good security, and desired use cases would obviously be listed as part of that process, but also any specifically disallowed use case should be considered and documented.

The following techniques should also be used:

Manually review with staff to test their understanding of security processes and policy, and to find out if they have the appropriate skills to design a secure application.

Threat Modelling requires an understanding of the attacker’s view of the system, but having a good threat model doesn’t mean you will find any of the flaws in the code.

A source code reviewer is looking for flawed business logic, access control problems, cryptographic weaknesses, as well as openings for malicious code. This is a complete, effective, fast, and accurate testing tool, but has the disadvantage of requiring highly skilled security developers.

Also known as ‘ethical hacking’, Penetration Testing can be done using automated testing tools. Although its probably the most popular form of testing, like Threat Modelling it may not identify the security flaw.

Manual Review, Threat Modelling, Source Code Review, and Penetration Testing should all be used in balance, as any one technique on its own will not cover all potential issues. These techniques must be initiated from the beginning of the application development process, otherwise some techniques will become impossible towards the end of development, or fixing errors that have been in existence for some time will become more expensive.

It could be said, since none of these processes or techniques were followed (aside from a small amount of source code reviewing), that the web application completed for the previous TMA case study has already failed all security tests.

The proprietors will have to make a call as to how much to spend on security. They will need to understand the risks of not spending anything, and the different levels of security that can be attained vs. the money available to spend on security. A small web application like Aficionados will not cost much to test, and identified vulnerabilities will need to be documented in a way that the gamers can understand, so they can decide how much more they want to spend on improving the code to plug the security gaps.

As Testing Objectives are specified by security requirements, and since the app uses SQL, SQL Injection is therefore a vulnerability, and must be tested against. A black box test might be used, followed by manual attacks.

Identity theft could also be a risk, so vulnerabilities in authentication, cryptographic controls, input validation and authorization controls need to be identified and tested.

Security requirements need to be function driven and they need to highlight the expected functionality and implicitly the implementation.

Some more specific processes to establish could be:

* Describe a Functional Scenario, where the user successfully authenticates. Then describe a Negative Scenario where an attacker breaks authentication.
* Mask confidential data in display.
* Only allow passwords that are alphanumeric, include special characters and six characters minimum length, to limit the attack surface.
* Error messages must be generic.
* Lock out accounts after reaching a log on failure threshold and enforce password complexity to mitigate risk of brute force password attacks.

1. Discuss the impact and importance of availability for an e-commerce enabled web application. What would you consider to be a limitation with this model in terms of today’s web applications?

Availability of an e-commerce enabled web application is very important. It makes no difference whether your target audience are local to New Zealand, or international, if time zones are what developers are concerned with, because customers in New Zealand are easily capable of using web applications at 3am just as much as at 9am or 4pm or any other time of the day. There will be spikes of demand when traffic could be heavy, but just like any road in the country, someone is always going somewhere.

Maintaining that constant availability requires all components of the app’s information system to work together seamlessly at all times. According to the Panmore Institute’s CIA Triad concept, Availability hinges on Confidentiality and Integrity of data and information systems. Confidentiality, Integrity, and Availability dovetail into each other so much that you can’t have one without the other functioning perfectly. And as confidentiality and integrity are all about properly established and well-maintained security, we could say that solid security guarantees availability.

I’m not convinced that one side of the triangle is more important than any other. The sides of any triangle are completely dependent on each other. It doesn’t matter how secret the secret is, its still a secret and access must be controlled. Its not relevant whether data integrity is life-threatening or not, because you still have to maintain perfect data, and designing a system that allows mistakes is never acceptable. And it doesn’t matter how secure your system is if the information can’t be accessed when the user requires it.

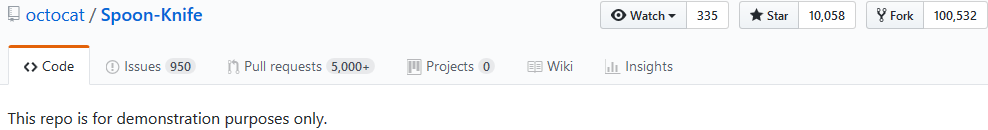
In terms of limitations of the CIA Triad compared to today’s web applications, current articles on the topic are older than March 2017 when the Panmore Institute’s article was last modified. Having said that, articles from 2015/2016 do suggest some issues that are extra to the concept proposed by Panmore Institute.

Resource conflicts can seriously limit availability, but are not directly related to data integrity or confidentiality. The level of training received by any help desk staff could also impact on availability, and while there is a security element involved in the job, the skill level of the staff is not directly security related. Rather than pay high fixed costs to maintain system speed, use a scalable system that can quickly amp up to meet heavy traffic spikes and only pay for high demand when its actually in demand (reducing cost is high on most company’s priority lists).

There is a school of thought that moving into The Cloud automatically improves all three sides of the triangle, but I can say from personal experience observing a large corporate system transition to the cloud a few months ago, the opposite can easily be true. Asking their IT department when things would improve, I was told “Get used to it – this is as good as it gets”. While they believe they have maintained Confidentiality and Integrity, they have certainly reduced Availability.

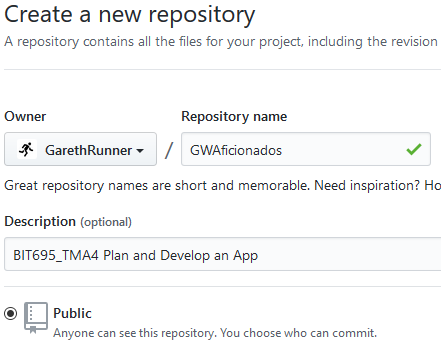
Task 2: Version control

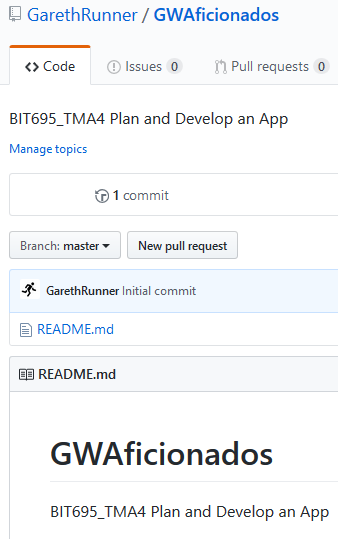
1. Post screenshots showing forking of demo repository.



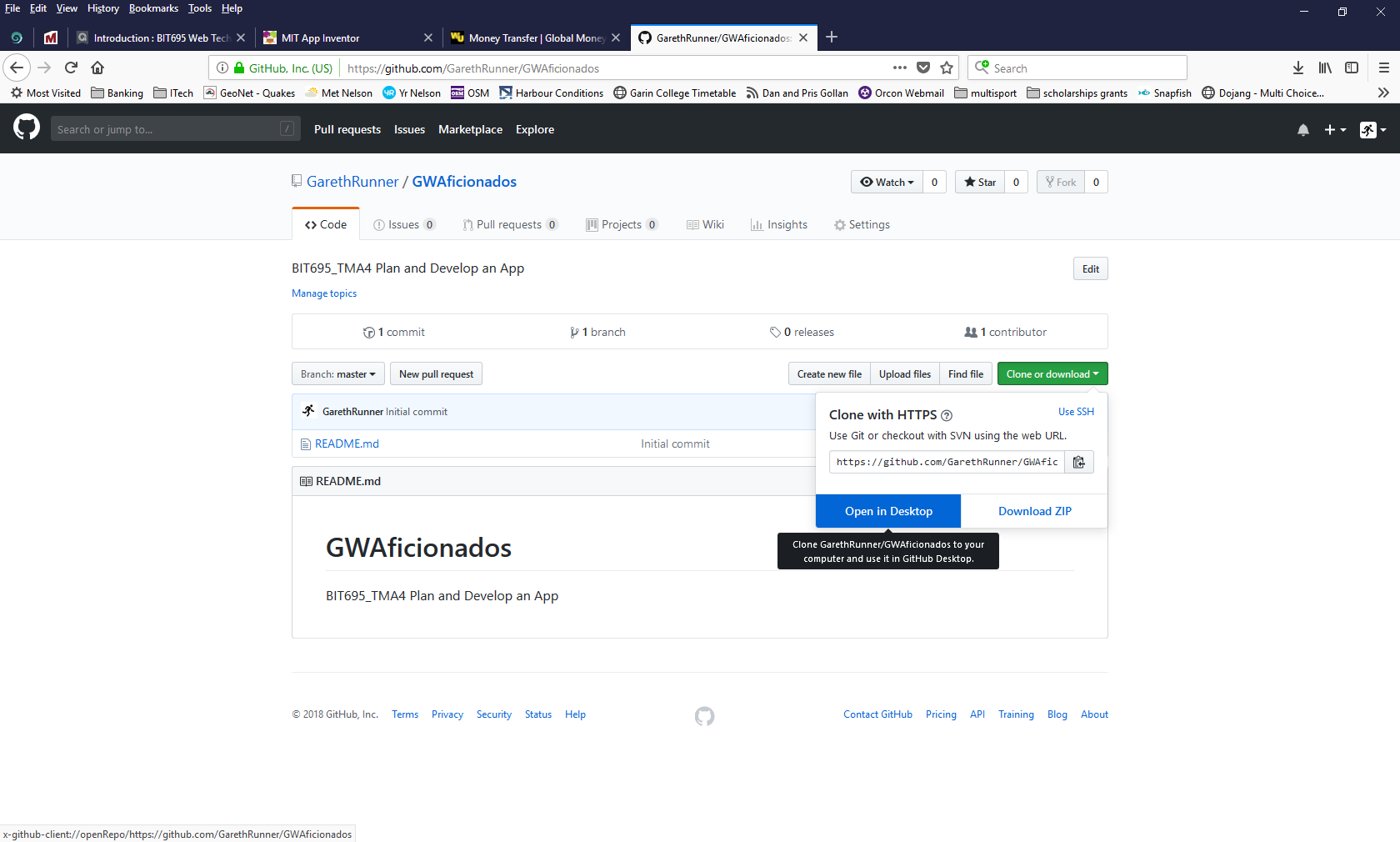
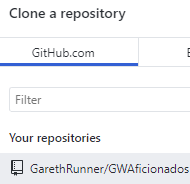


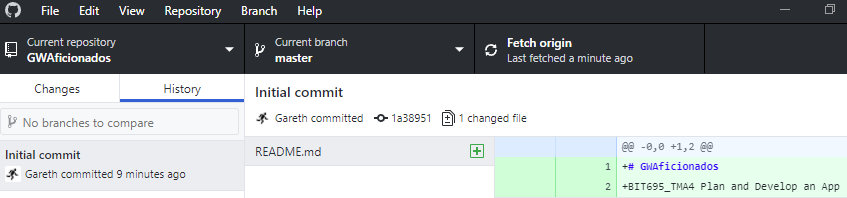
1. Post screenshots showing creation of a new repository, connection with desktop version, and cloning of *freeCodeCamp*.

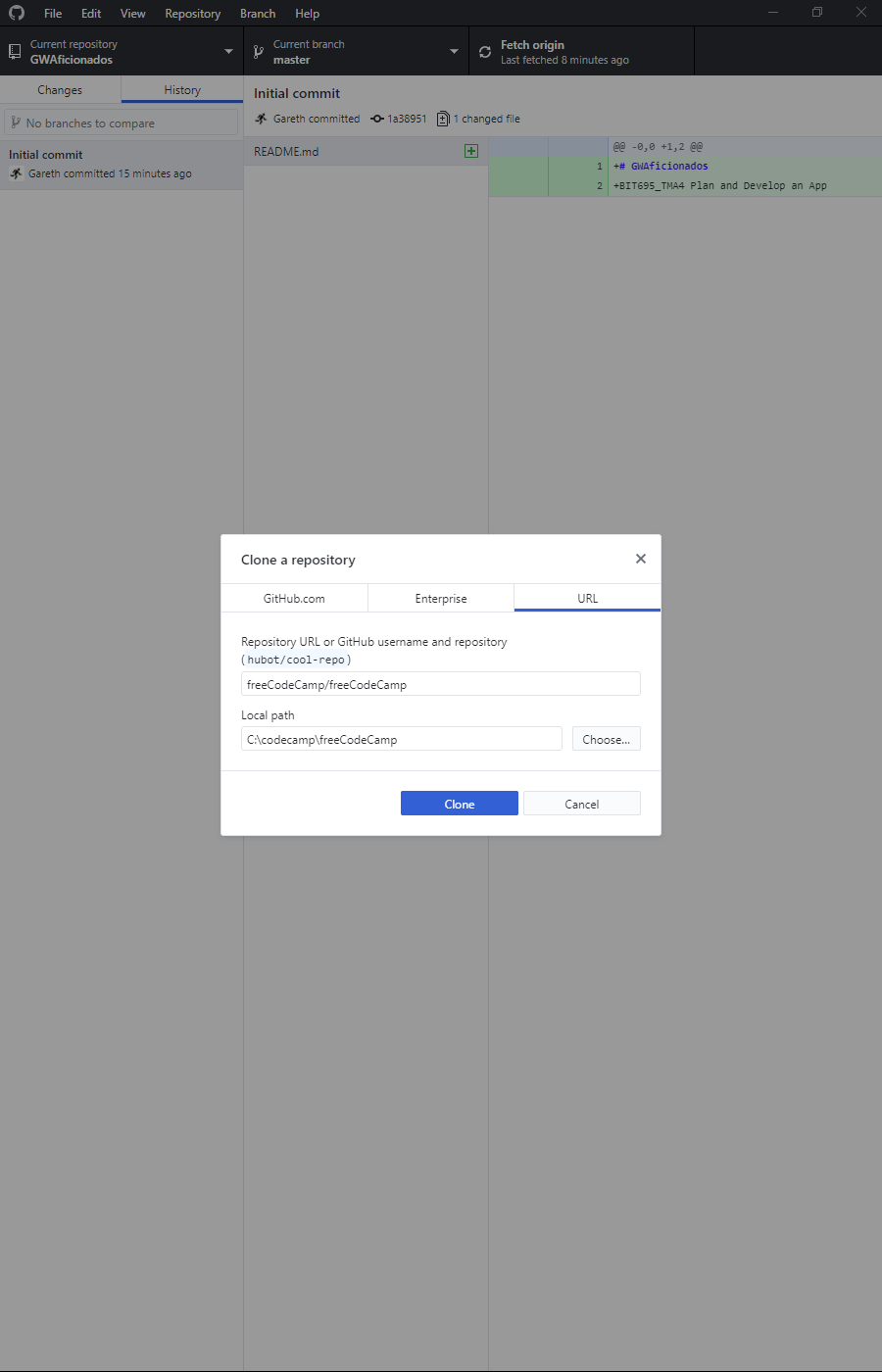


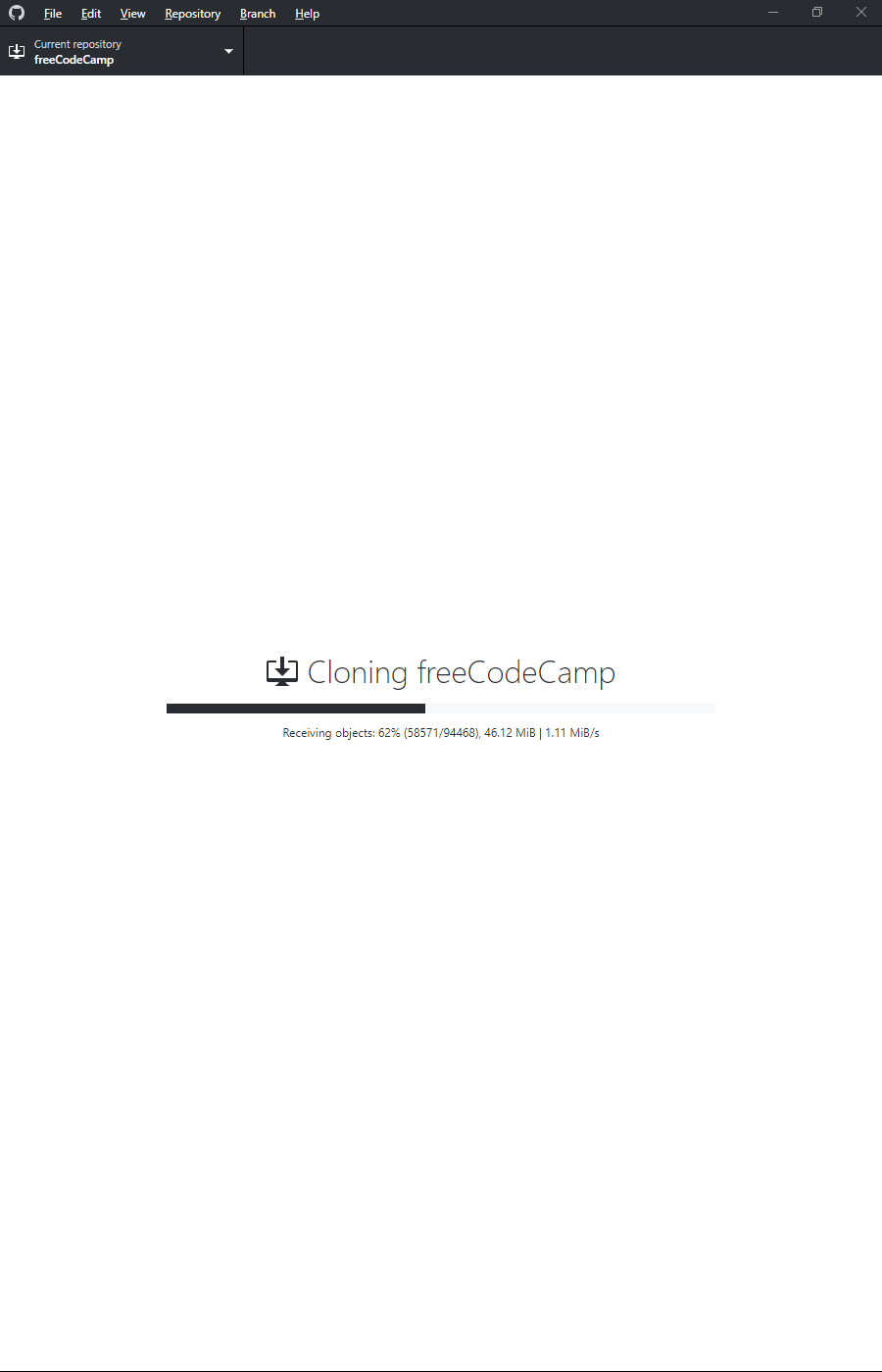


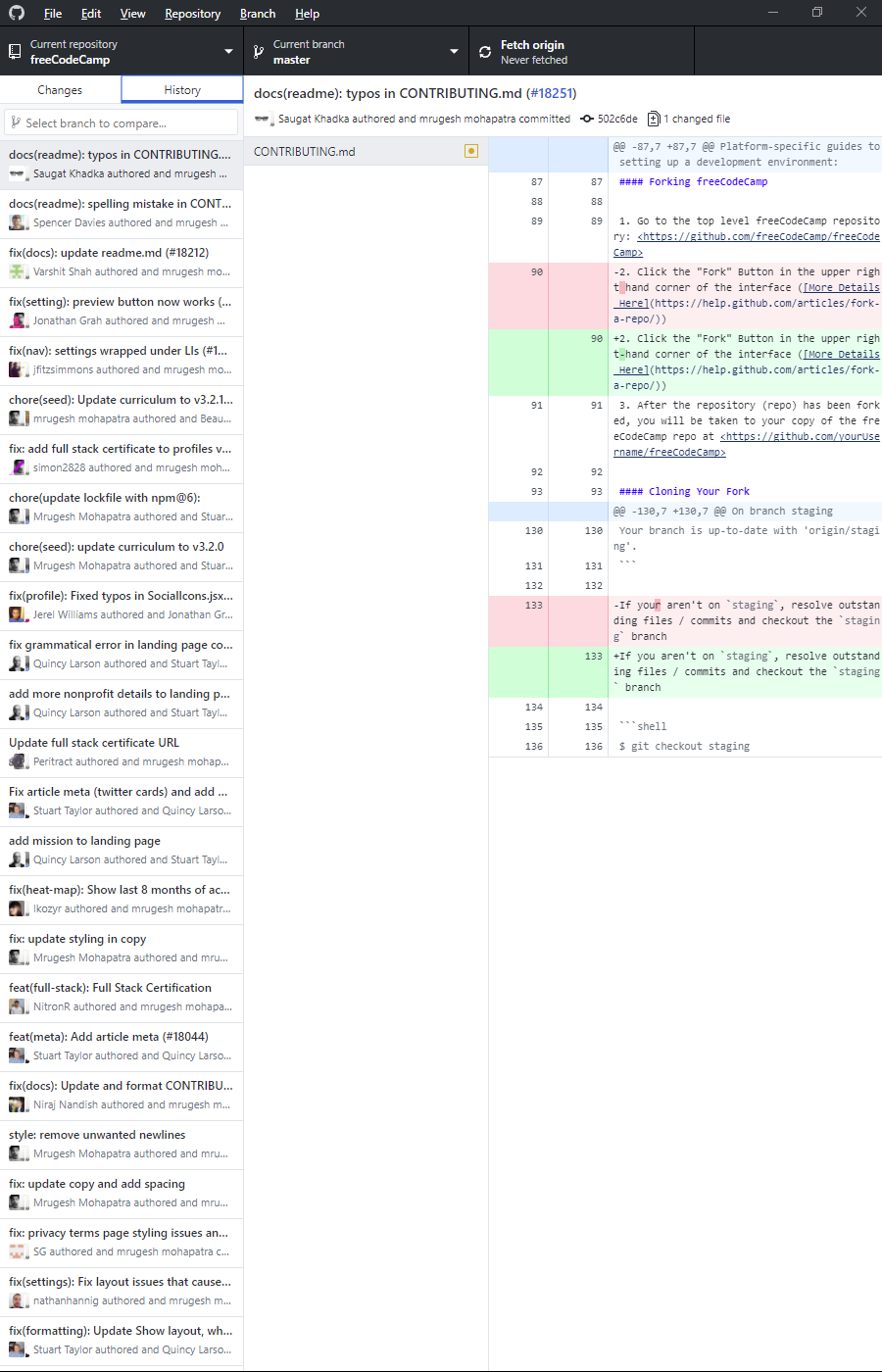
Two options:

 or 









1. Compare Github and Bitbucket. Use table form and compare at least 10 features.

|  |  |  |
| --- | --- | --- |
| Feature | GitHub | Bitbucket |
| Common to both | Pull request, Code review, Inline editing, Issue tracking, Markdown support, Two-factor authentication, Advanced permission management, Hosted static web pages, Feature-rich API, Fork/Clone repositories, Snippets, 3rd party integrations | |
| Private repos | None free (unlimited for $7/mth per user). | Unlimited. No charge. Conditions are that there be no more than 5 users, and restricted to 50 min/month of builds and 1 Gb/month of storage. |
| Integrations | Direct integration with Zendesk, Cloudbees, Travis, AWS, Codeclimate, Azure, Google Cloud, Heroku | Direct integration with Bamboo, Jira, Crucible, Jenkins |
| Price (cost for an average of 50 users working with private repositories over the course of a year) | $8000.  Enterprise level could cost $20,000. | $1860. Cheaper since its free up to 5 users, and offers unlimited private repos. Enterprise level could cost $6000. |
| Mercurial | Not supported | Only Bitbucket can work with Mercurial |
| SVN | Supports SVN clients | Not supported |
| Extras | Syntax highlighting | Supports external authentication with GitHub, Facebook, Twitter and Google |
| Import | Import repos easily from Git, SVN, HG, TFS | Import repos easily from Git, SVN, HG, Codeplex, Google Code, SourceForge |
| Integration with Jira | Works. | “Blows GitHub out of the water”. Easier implementation, more coherent workflows, leverage more tools more easily, code a better product. |
| Integration with Jenkins | Build Integration and Authentication Integration are both easier with GitHub. | Works. |

Task 3: Application planning and development

1. Create a schedule of activities and a risk assessment.

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Start date and time** | **Expected completion date and time** | **Notes or comments** |
| Complete Block 4 | 6 OCT 22:00 | 14 OCT 23:30 |  |
| Add missing database tables | 12 OCT 22:00 | 13 OCT 23:30 |  |
| Code supporting CRUD | 14 OCT 22:00 | 17 OCT 23:30 |  |
| Test and Check | 18 OCT 22:00 | 18 OCT 23:30 |  |
| Submit TMA | 18 OCT 23:45 | 18 OCT 23:50 | Heading into the mountains Labour Weekend, no internet access, so must submit Thu night! |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk event** | **Impact** | **Mitigation steps** | **Severity (1-5)** |
| Missed deadline | Failure of app, potential loss of 40 points | Work through the night(s) | 2 |
| Hardware failure | Unable to proceed, loss of $1000 asset | Wait for Noel Leeming to open and buy new PC | 1 |
| Lack of technical knowledge | Failure of app, potential loss of 40 points | Call for help with understanding missed concepts | 2 |
| Behind schedule | No time to test and check, potential loss of some points | Work through the night(s) | 4 |
| Internet down | Unable to submit TMA | If still down past deadline then advise OP team at first opportunity and submit | 3 |

1. Develop SQL code that creates the remaining 4 tables.

Submitted as file “initiate.sql” in the BIT695 directory.

1. Create HTML, CSS, and PHP for the CRUD forms supporting the new set of tables. Focus on the relationship between the board games table and the board games assigned to a player (develop a form facilitating the joining of these two tables).

Submitted as the rest of the files in the BIT695 directory.