Agility 2018 Hands-on Lab Guide

Contents:

1

Class 1: Introduction to Fraud and F5 WebSafe

Welcome to the Introduction to Fraud and F5 WebSafe Agility hands-on lab session. These labs are intended to show you the dangers of both malware and phishing, and how F5 WebSafe helps organizations with fraud detection and protection. This guide is intended to complement lecture material provided during the Introduction to Fraud session as well as a reference guide that can be referred to after the class as a basis for troubleshooting malware, phishing, and WebSafe in your own environment.

1.1 Lab Network Setup

In the interest of focusing as much time as possible seeing malware and phishing detection and protection in action, we have provided some resources and basic setup ahead of time. These are:

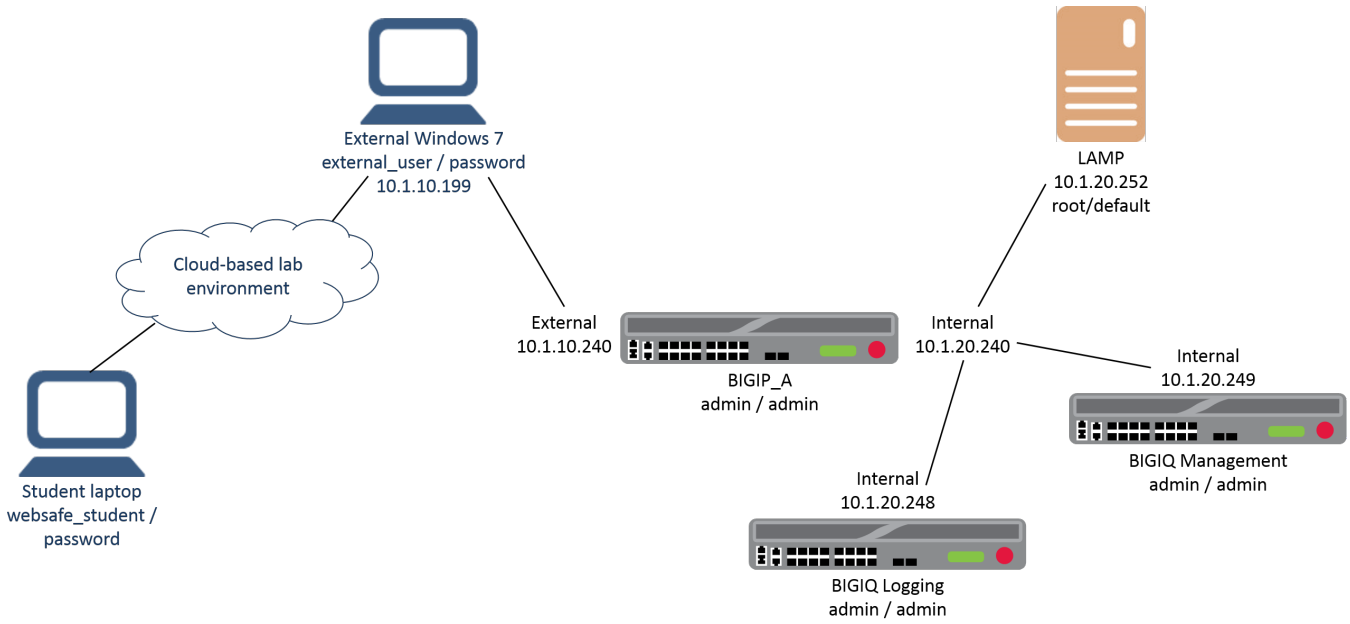
- Cloud-based lab environment complete with an infected Windows workstation, a virtual BIG-IP (VE), a virtual BIG-IQ acting as a logging node, a virtual BIG-IQ acting as a management node, and a back-end banking application running on a Linux web server.
- The virtual BIG-IP has been pre-licensed and provisioned for WebSafe

If you wish to replicate these labs in your office you will need to perform these steps accordingly. Additional lab resources are provided as illustrated in the diagram on the next page.

To access the lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the lab training portal. The RDP client will be used to connect to a Windows workstation, where you will be able to access the BIG-IP and BIG-IQ management interfaces (HTTPS, SSH).

You class instructor will provide additional lab access details.

1.1.1 Lab Diagram



1.1.2 Timing for Labs

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. This can never be accurately predicted but we strived to derive an estimate among several people each having a different level of experience. Below is an estimate of how long it will take for each lab:

LAB Name (Description)	Time Allocated
LAB 1 – Examine the Dangers of Malware and Phishing)	25 minutes
LAB 2 – Use Malware Detection)	30 minutes
LAB 3 – Use Phishing Detection	30 minutes
LAB 4 – Use Application Layer Encryption	30 minutes

1.2 Module 1: F5 WebSafe Introduction

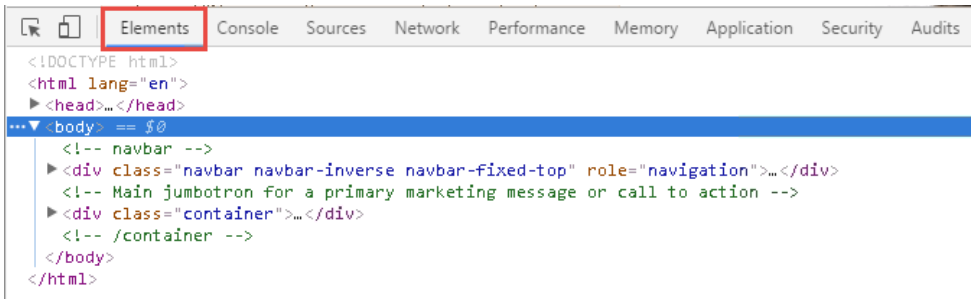
1.2.1 Lab 1: Examine the Dangers of Malware and Phishing

In this lab, you will see how malware can manipulate web pages using the Document Object Model (DOM), and then you will see how easy it is to create a phishing web site:

Task 1 - Connect to Ravello and Use Chrome to Manipulate a Web Page

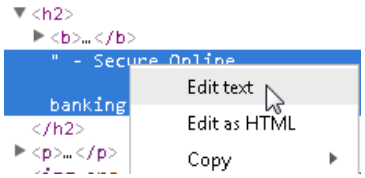
1. Use a browser to access **http://IP_address** with the IP address supplied by your instructor, and log in using the username and password supplied by your instructor.
2. For **WebSafe Training Blueprint** click **View**.
3. Copy the IP address of the **Windows 7 External** VM, and then use RDP to access the IP address.

4. Log into the Windows workstation as **external_user** / **password**.
5. Update the Windows time:
   (a) Select the clock and click **Change date and time settings...**
   (b) Select the **Internet Time** tab, and then click **Change settings...**
   (c) Select **time.windows.com**, and then click **Update now**.
6. Open Chrome and press the **F12** key, and then click the **Bank** bookmark.
7. Examine the **Elements** tab.



   The **<html>** element is the top-level of the document object model tree. This element contains two child nodes, **<head>** and **<body>**, and the **<body>** node contains two ** ** child nodes.
8. Expand the second ** ** node, and then expand its child ** ** node.
9. Mouse-over the second child ** ** node and examine the web page.

   This element represents the Demo Bank heading and the text below it.
10. Expand the second child ** ** node, then mouse over the **<h2>** element and the **<p>** element and examine the web page.
11. Expand the **<h2>** node, then right-click on **" – Secure Online**, and then select **Edit text**.



12. Edit the element from **– Secure Online** to **– Very Insecure Online**, then press the **Enter** key.
13. Examine the change to the web page.

    You've just made a simple change to the web page within the browser after it was sent from the web server.
14. Copy the following text:

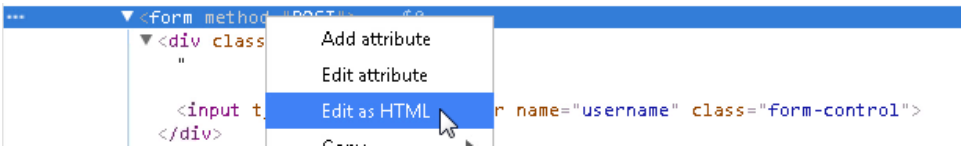
```
<form method="POST">
<div class="form-group">
  Username: <input type="text" placeholder="" name="username" class="form-control
↪">
</div>

<div class="form-group">
  Password: <input type="password" placeholder="" name="password" class="form-
↪control">
</div>
```

```
<div class="form-group">
  ATM Pin: <input type="text" placeholder="" name="pin" class="form-control">
</div>

<input type="submit" class="btn btn-success" style="float:right" value="Login">
</form>
```

15. In the web page, right click inside the **Username** field and select **Inspect**.
16. Right-click the **<form method="POST">** line, and then select **Edit as HTML**.



17. Select and delete all the text between the **<form>** opening tag and the **</form>** closing tag, then paste the text that copied to your clipboard earlier, then click outside of the **<form>** editing area and examine the web page.
18. Enter the following credentials but do not click **Login**. **Username**: your first name **Password**: P@ssw0rd! **PIN**: your last name
19. In the inspection window open the **Console** tab, and in the console, one at a time type (or copy and paste) each of the following and press **Enter**:

```
document.forms[0].username.value

document.forms[0].password.value

document.forms[0].pin.value
```

These values haven't yet been submitted and are therefore available in cleartext for form grabbing.

20. In the console, one at a time type (or copy and paste) each of the following and press **Enter**:

```
document.forms[0].username.value = "bob"

document.forms[0].pin.value = "smith"
```

21. Examine the web page form.

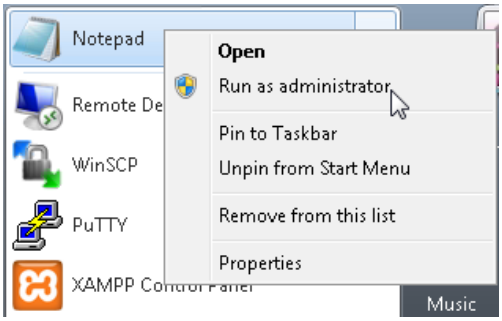
Malware can manipulate the parameter values before they are submitted.

22. Click the **Bank** bookmark, then click the **Demo Tools** bookmark, and from the Demo Tools click **Start Keylogger**, and then click on the **Password** field.
23. For **Password** type **P@ssw0rd1** and examine the top of the Demo Tools window.

A keylogging program can capture the characters of the user's password as they're typed.

Task 2 - Create a Phishing Web Site

1. Open the **Start** menu, then right-click on **Notepad** and select **Run as administrator**, and then click **Yes**.

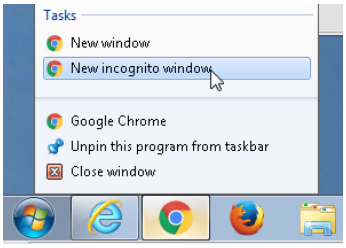


2. Go to **File > Open**, from the file types list select **All Files**, and then open the **hosts** file.
3. At the end of the hosts file list, add a new entry for the following, and then save and close the **hosts** file.

   ```
   10.1.10.16 bank.vlab.f5demos.com
   ```

4. In the banking page click the **Bank** bookmark.
5. Right-click inside the page and select **Save as**.
6. Navigate to the desktop and open the **Phishing** directory.
7. Name the file **login.html**, ensure that **Webpage, Complete** is selected and click **Save**, and then close the banking page.
8. Open **WinSCP**.
9. Change the **File protocol** to **SCP**, for **Host name** type **10.1.1.252**, and log in as **root** / **default**.

   This is a web server that's been high jacked by a phishing hacker.
10. In the left panel for the Windows workstation, navigate to the desktop and open the **Phishing** directory.
11. In the right panel for the high-jacked web server, navigate to **var/www/dvwa**.
12. Select both **login.html** and **login_files** and copy them into the **dvwa** directory, and then close **WinSCP**.
13. Open an incognito window and access **http://bank.vlab.f5demos.com/login.html**.



14. Enter the following credentials and click **Login**. **Username**: your first name **Password**: P@ssw0rd!

Note: Your login fails, however you have just submitted your username and password on the hacker's phishing site.

---

15. Close Chrome.

Task 3 - Configure BIG-IQ for Logging

1. Open Chrome and click the **BIGIQ_Mgmt** bookmark, and then log into the BIG-IQ system as **admin** / **admin**.
2. On the **BIG-IQ Logging > Logging Nodes** page click **Add Node**.
3. Use the following information, and then click **Add**.

Form field	Value
IP Address	10.1.20.248
User name	admin
Password	admin
Transport Address	10.1.20.248
Transport Port	9300

   It takes a couple of minutes to discover the logging node.

4. Once the logging node has been discovered, click **bigipqlogging.f5demo.com**, and then open the **Services** page.
5. For **Fraud Protection Service**, click **Activate**.
6. Once the activation is complete, open a new tab and click the **BIGIP_A** bookmark, and then log into the BIG-IP system as **admin** / **admin**.
7. Open the **Pool List** page and ensure that the **bigiq_logging_pool** displays as online.

1.2.2 Lab 2: Use Malware Detection

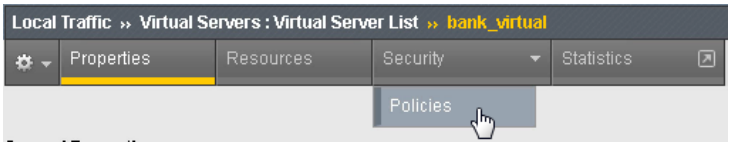
In this lab, you will see how to create and configure a BIG-IP WebSafe anti-fraud profile and see how malicious activity sends alerts to the BIG-IQ logging server for viewing and analysis.

Task 1 - Create a WebSafe Anti-Fraud Profile

1. In the BIG-IP Configuration Utility, open the **Security > Fraud Protection Service > Anti-Fraud Profiles** page and click **Create**.
2. Use the following information, and then click **Create**.

Form field	Value
Profile Name	banking_fraud_profile
Alert Identifier	D1 (you need to first click the checkbox to the right of the field)
Alert Pool	bigiq_logging_pool (same note as above)
Log Publisher	bigiq_logging_publisher (same note as above)

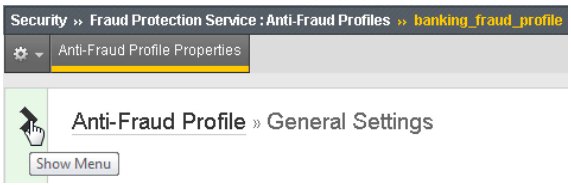
3. Open the **Virtual Server List** page and click **bank_virtual**, and then open the **Security > Policies** page.



4. From the **Anti-Fraud Profile** list select **Enabled**.

5. From the **Profile** list select **banking_fraud_profile**, and then click **Update**.
6. Open a new tab and press the **F12** key, and then click the **Bank** bookmark.
7. In the inspection window examine the files on the **Network** tab.

   There are five files returned from the web server to build this web page.
8. In the BIG-IP Configuration Utility, open the **Security > Fraud Protection Service > Anti-Fraud Profiles** page and click **banking_fraud_profile**.
9. Expand the left panel and click **URL List**, and then click **Add**.



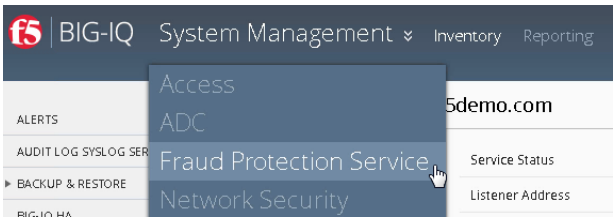
10. For **URL Path** leave **Explicit** selected, and type /**login.php**.
11. Expand the left panel and open the **Malware Detection** page.

    Note that nearly all malware detection options are enabled by default.
12. Click **Create**.
13. In the banking tab click the **Bank** bookmark and examine the **Network** tab.

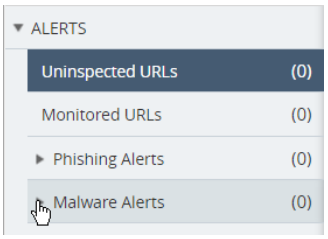
There is now a **script** file and additional files that were added by BIG-IP WebSafe.

Task 2 - View WebSafe Alerts

1. In the BIG-IQ Configuration Utility, from the main BIG-IQ menu select **Fraud Protection Service**.

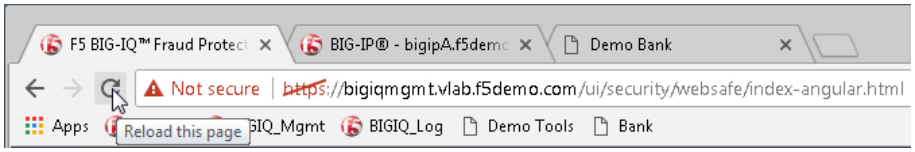


2. On on the left panel open the **Malware Alerts** section.



   No alerts have been generated yet.
3. In the banking tab click the **Demo Tools** bookmark and then click **Insert Malicious Script**.
4. For the **Malicious domain** field, copy and paste **http://www.hackingsite.com/inject.js**, and then click **OK**.
5. Log in as **bobsmith** / **P@ssw0rd1**, and then click **Logout**.

6. In the BIG-IQ Configuration Utility reload the page, then open the **Malware Alerts > External Scripts** page, and then expand the **hackingsite.com** alert.



An external script has been reported with the alert type of **External Sources**. There are also additional alerts caused by the **Demo Tools** bookmark, which also makes calls to scripts from external sources.

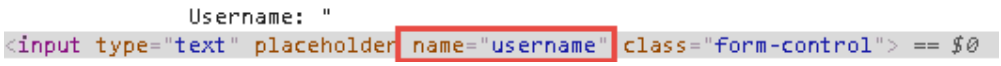
7. Examine the **User Name** column.

   The user name is presently **Unknown**.

8. Expand the alert section for **ajax.googleapis.com** and select the alert checkbox, and then click **Remove** and then **Delete Selected**.

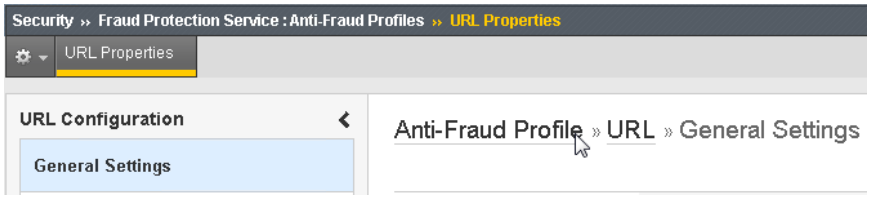
9. Repeat the step above for the alert for **s3-eu-west-1.amazonaws.com**.

10. In the banking tab, to discover the parameter name that needs to be sent to the alert server, right-click inside the **Username** field and select **Inspect**.

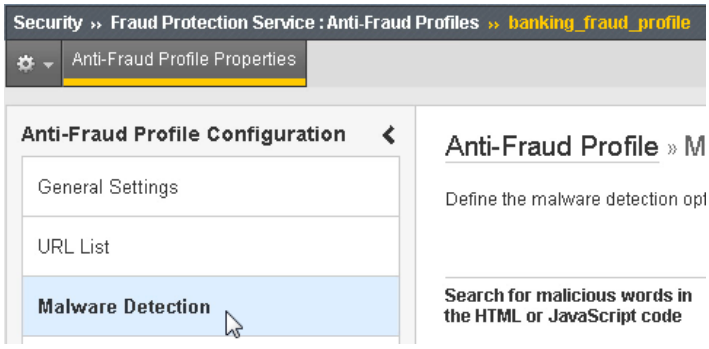


   The parameter name is `username`.

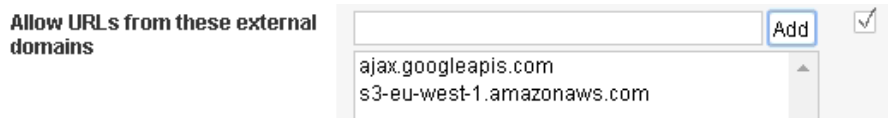
11. In the BIG-IP Configuration Utility, for the `banking_fraud_profile`, click the `Anti-Fraud Profile` link (see below).



12. From the left panel select the global **Malware Detection** option.

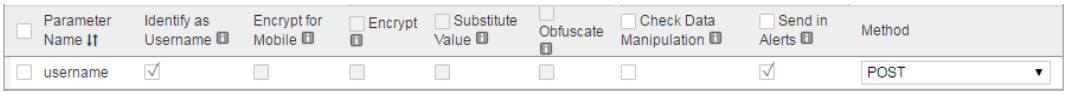


13. For **Allow URLs from these external domains**, add both **ajax.googleapis.com** and **s3-eu-west-1.amazonaws.com**, and then click **Save**.



14. From the left panel select **URL List**, and then click /**login.php**.
15. From the left panel select **Login Page Properties**, and then select the **URL is Login Page** checkbox.
16. For **Expected HTTP response status code**, in the **Specify** field enter **302**.

17. From the left panel select **Parameters**.
18. Create a new parameter named **username**, and then click **Add**.
19. Select the **Identify as Username** and **Send in Alerts** checkboxes, and then click **Save**.



20. In the banking tab click the **Bank** bookmark, then click the **Demo Tools** bookmark and click **Insert Malicious Script**.
21. For the **Malicious domain** field, copy and paste **http://www.worsesite.com/malware.js**, and then click **OK**.
22. Log in as **bobsmith** / **P@ssw0rd1**, and then click **Logout**.
23. In the BIG-IQ Configuration Utility reload the page, and then in the **Malware Alerts > External Scripts** section expand the **worsesite.com** alert.

    The user name information (**bobsmith**) is now being sent to the alert server. In addition, the scripts used for the Demo Tools are no longer triggering alerts. (NOTE: If the **User Name** is still displaying as **Unknown**, wait about 30 seconds and reload the page again.)

Task 3 - Check for Malware JavaScript Signatures

1. In the BIG-IQ Configuration Utility open the **Malware Alerts > Alert Transform Rules** page and click **tatang.Trojan**.

   This signature, looking for **tatangakatanga**, was added before the exercise. Notice at the bottom of the page the alert severity is configured at **90**.
2. In the BIG-IP Configuration Utility, click the `banking_fraud_profile` **Anti-Fraud Profile** link, and then from the left panel open the global **Malware Detection** page.
3. For the **Search for malicious words in the HTML or JavaScript code** field, add both **tatangakatanga** and **trojan** as two separate entries to the global forbidden list, and then click **Save**.
4. Select **URL List** and click /**login.php**.
5. From the left panel select **Malware Detection** and scroll down to the **Malware JavaScript Signatures** option.

   By default, words added to the global list are configured for all URLs. Notice you could ignore a globally defined JavaScript signature for a specific URL.
6. In the banking tab click the **Bank** bookmark, then click the **Demo Tools** bookmark and then click **Imitate Trojan**.

This imitates a trojan for **tatangakatanga**.

7. Log in as **bobsmith** / **P@ssw0rd1**, and then click **Logout**.
8. In the BIG-IQ Configuration Utility reload the page, and then open the **Malware Alerts > Targeted Malware** page and expand the **bobsmith** grouping.

   A **tatang.Trojan** alert was issued. Notice the severity level of **90**. In addition, a **Symbols Found** alert was issued, due to the word **trojan** that occurred when you clicked **Imitate Trojan**.

Optional Task - Require Mandatory Words

1. In the BIG-IP Configuration Utility, open the **URL List** page and click /**login.php**.
2. From the left panel select **Malware Detection**.
3. In the **Mandatory Words** section, add both **Secured** and **We will never ask you** as two separate entries to the mandatory words list, and then click **Save**.
4. In the banking tab click the **Bank** bookmark, then log in as **bobsmith** / **P@ssw0rd1**, and then click **Logout**.
5. In the BIG-IQ Configuration Utility reload the page, and then open the **Validation Errors > Missing Components** page, and then expand the alert.

   A **String(s) Are Not Visible** alert was issued.
6. Click **String(s) Are Not Visible** and view the **Alert Details**.

   The alert was issued due to the missing words **Secured**.
7. Click **Remove** and then **OK**, and then click **Refresh**.
8. In the banking tab, examine the Demo Bank page.

   The word that appears at the top of the page is actually **Secure**, not **Secured**.
9. In the BIG-IP Configuration Utility, select the **Secured** entry and click **Delete**, and then add a new entry for **Secure**, and then click **Save**.
10. In the banking tab click the **Bank** bookmark.
11. In the BIG-IQ Configuration Utility reload the page, and then open the **Validation Errors > Missing Components** page.

No new alerts were generated.

1.2.3 Lab 3: Use Phishing Detection

In this lab, you will add phishing detection to the banking application, then redo the task of adding the phishing site to the high-jacked server, and then view alerts triggered when the phishing site is accessed.

Task 1 - Enable Phishing Detection

1. Open an incognito window and access the phishing web site at **http://bank.vlab.f5demos.com/login.html**.
2. Enter the following credentials and click **Login**. **Username**: your first name **Password**: P@ssw0rd!
3. Close the phishing page.
4. In the BIG-IQ Configuration Utility reload the page, then open the **Phishing Alerts > Phishing** page.

   There are no alerts because this page was copied before a WebSafe profile was added to the virtual server.
5. In the BIG-IP Configuration Utility, select the `login.php` from the **URL** page, and then from the left menu select **Phishing Detection**.

When you created the WebSafe profile, phishing detection was enabled by default.

Task 2 - Detect Phishing of a Web Site

1. From the desktop open the **Phishing** directory and delete the two files you created earlier.
2. In the banking tab click the **Bank** bookmark, then right-click inside the page and select **Save as**.
3. Name the file **login.html**, ensure that **Webpage, Complete** is selected and that you're saving into the **Phishing** directory and click **Save**, and then close the banking tab.
4. Open **WinSCP**.
5. Change the **File protocol** to **SCP**, for **Host name** type **10.1.1.252**, and log in as **root** / **default**.
6. In the left panel for the Windows workstation, navigate to the desktop and open the **Phishing** directory.
7. In the right panel for the web server, navigate to **var**/**www**/**dvwa**.
8. Delete the two files currently in the **dvwa** directory.
9. Select the new **login.html** and **login_files** and copy them to the **dvwa** directory.
10. Open a new incognito window and access **http://bank.vlab.f5demos.com/login.html**.
11. Attempt to log in as **bobsmith** / **P@ssw0rd1**, and then close Chrome.
12. In the BIG-IQ Configuration Utility reload the page, then open the **Phishing Alerts > Phishing** page, and then expand the **bank.vlab.f5demos.com** alert.

    A **Copied Pages** alert was generated, and in addition a **Phishing Users** alert was generated for user **bobsmith**.
13. Click **Copied Pages** and view the **Domain** and the **Additional Info**.

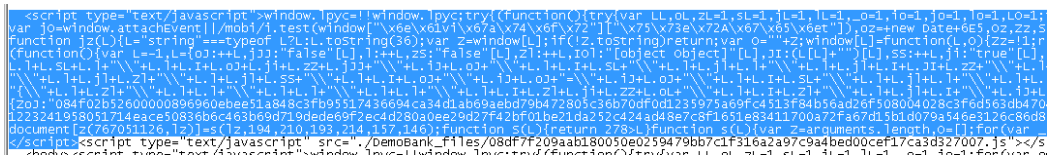
The fake domain name is **bank.vlab.f5demos.com** and the original page is **https://bank.vlab.f5demo.com/login.php**.

Task 3 - Use JavaScript Removal Detection

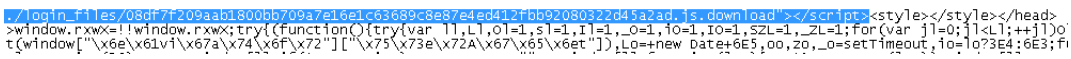
1. In WinSCP, in the **dvwa** directory, right-click **login.html** and select **Edit**.
2. Click on the find (binoculars) button and type **<script** and click **Find Next** several times to locate all scripts in the page.

   There are three script entries added by WebSafe.

3. Select and delete everything from the first **<script type="text/javascript" src=. . . >** tag to its closing **</script>** tag.



4. Select and delete everything from the next **<script type="text/javascript">** tag to its closing **</script>** tag (right before the **<style>** tag near the end of the same line).



5. Select and delete everything from the final **<script type="text/javascript">** tag to its closing **</script>** tag (right before the **<img home= >** tag).
6. When you're done, your code should resemble the following:

```
                padding-bottom: 20px;
            }
        </style>

<style></style></head>
<body><img home="https://bank.vlab.f5demo.com/DALRL8/?id=D1&amp;c=im&amp;phg=HXie72t31zI3"

    <!-- navbar -->
```

7. Save and close the **login.html** file.
8. Open a new incognito window and access **http://bank.vlab.f5demos.com/login.html** and attempt to log in as **bobsmith** / **P@ssw0rd1**, and then close Chrome.

Notice the page still displays as expected.

1. In the BIG-IQ Configuration Utility reload the page, then open the **Phishing Alerts > Advanced Phishing** page, and then expand the **bank.vlab.f5demos.com** alert.

   Although the hacker removed the JavaScript, a **CSS Check** alert and an **Image Check** alert was issued.

2. Close **WinSCP**.

1.2.4 Lab 4: Use Application Layer Encryption

In this lab, you will add application layer encryption in addition to several other features that help to protect sensitive web applications.

Task 1 - View the Application Before Enabling Application Layer Encryption

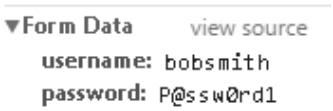
1. Open a new Chrome window and press the **F12** key, then click the **Bank** bookmark.
2. Enter the credentials **bobsmith** / **P@ssw0rd1** but do not click **Login**.
3. In the inspection window open the **Console** tab, and in the console, type (or copy and paste) the following and press **Enter**:

   ```
   document.forms[0].password.value
   ```

   This value hasn't yet been submitted and is therefore available in cleartext for form grabbing.

4. In the inspection window open the **Network** tab and select the **Preserve log** checkbox.

5. Log in as **bobsmith** / **P@ssw0rd1**.
6. In the inspection window, click the second **Login.php** entry, and then in the **Headers** tab scroll down and examine the **Form Data** section.



   Both the username and the password are in cleartext. They are both currently vulnerable to a hacker or a malware script.
7. Click **Logout**, and then right-click inside the **Password** field and select **Inspect**.
8. While you examine the **Elements** tab, for **Password** type **P@ssw0rd1**.

   Encryption is not taking place in real-time, making it vulnerable to malware that grabs passwords as they're typed.
9. Click the **Bank** bookmark, then click the **Demo Tools** bookmark, and from the Demo Tools click **Start Keylogger**, and then click on the **Password** field.
10. For **Password** type **P@ssw0rd1** and examine the top of the Demo Tools window.

   The WebSafe application layer encryption keylogging protection adds multiple random characters as the user types their password, which will render the keylogging file useless.
11. Right-click inside the **Username** field and select **Inspect**, and then examine the **name** value for this input parameter.

   You can view the name for this parameter: **username**. You can also view the name of the password parameter. This makes it easy for the fraudsters to craft targeted malware and create mass attacks.
12. Right-click the **<form method="POST">** line, and then select **Edit as HTML**.

   The code within the form is static HTML. There are three parameters, the username and password fields and the submit button. This static HTML code makes it very easy for malware to manipulate the page and extract values typed by the victim.
13. Close the Demo Bank page.

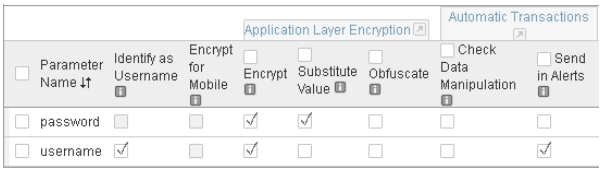
Task 2 - Enable Application Layer Encryption

1. In the BIG-IP Configuration Utility, from the left menu panel select **Application Layer Encryption**.

Notice that most options are currently selected.

1. From the left panel select **Parameters**, and for the **username** parameter select the **Encrypt** checkbox.

2. Create a new parameter named **password**, and then click **Add**.
3. For the **password** parameter select the **Encrypt** and the **Substitute Value** checkboxes, and then click **Save**.



Task 3 - View the Application After Enabling Application Layer Encryption

1. Open a new incognito window and press the **F12** key, then click the **Bank** bookmark.
2. Enter the credentials **bobsmith** / **P@ssw0rd1** but do not click Login.
3. In the inspection window open the **Console** tab, and in the console, type (or copy and paste) the following and press **Enter**:

   ```
   document.forms[0].password.value;
   ```

   The password value has been masked prior to the user submitting the web form. If the hacker thinks that this user's password is **A@aaa1aa1** they may attempt to log in as the victim.
4. Change the password BY TYPING **A@aaa1aa1** and click **Login**.
5. In the BIG-IQ Configuration Utility reload the page, then open the **Suspicious Logins > Stolen Credentials** page, and then expand the alert.

   A **Stolen Credentials** alert was issued.
6. In the banking page, right-click inside the **Password** field and select **Inspect**.
7. While you examine the **Elements** tab, for **Password** type **P@ssw0rd1**.

   Encryption for the password field is taking place in real-time, as you type.
8. In the inspection window open the **Network** page and select the **Preserve log** checkbox.
9. Log in as **bobsmith** / **P@ssw0rd1**.
10. In the inspection window click the second **Login.php** entry, and then in the **Headers** tab scroll down and examine the **Form Data** section.

Both the username and password parameter values are now encrypted after submitting the form.

Task 4 - Add Parameter and Form Obfuscation

1. In the BIG-IP Configuration Utility, from the left panel select **Application Layer Encryption**.
2. Select the **Add Decoy Inputs** checkbox.
3. Select **Parameters**, and for both the **username** and **password** parameters select the **Obfuscate** checkboxes, and then click **Save**.
4. In the banking page click **Logout**, and then click the **Bank** bookmark.

5. Right-click inside the **Username** field and select **Inspect**.
6. Examine the **name** value for this input parameter.

   The name of the username parameter is now obfuscated. In addition, the obfuscated value changes every few seconds.

7. Examine the values between the **<form method="POST">** line and the **</form>** line.

   WebSafe adds and removes decoy input fields in the HTML source code dynamically, making it virtually impossible for a fraudster to manipulate the form and/or steal data from it.

8. In the inspection window select the **Network** page, and then select the **Preserve log** checkbox.
9. Log in as **bobsmith** / **P@ssw0rd1**.

   The successful login shows that the HTML obfuscation works transparently and does not affect the user experience.

10. In the inspection window click the newest **Login.php** entry, and then in the **Headers** tab scroll down and examine the **Form Data** section.

    There is no longer any mention of the username or password parameters, and it now appears that there are several other parameters on the page.

That concludes the hands-on exercises for the Introduction to Fraud and BIG-IP WebSafe lab session.