

## Lab 4: Login Page Protection¶

In this final lab we will explore some of the login protection and session tracking capabilities present in F5 Advanced WAF and end with a fully configured Virtual Server. F5 Advanced WAF not only has the capability to gather user identity details from login pages and APM, but can also generate a unique Device-ID for each connected client.

### Virtual Server Configuration¶

1. Navigate to **Local Traffic > Virtual Servers > owasp-juiceshop\_443\_vs > Security > Policies** and enable the Application Security Policy: **juiceshop\_blocking**.
2. **Enable** the **Balanced\_Bot\_Profile** and add both the **Log all requests** and **Balanced\_Bot\_Log** logging profiles and click **Update**. You can leave the DoS profiles in place. Your fully configured Virtual Server config should look like this:

Local Traffic > Virtual Servers : Virtual Server List > **owasp-juiceshop\_443\_vs**

Properties Resources Security Statistics

**Policy Settings**

Destination	10.1.10.145:443
Service	HTTPS
Application Security Policy	Enabled... Policy: <b>juiceshop_blocking</b>
Service Policy	None
IP Intelligence	Disabled
DoS Protection Profile	Enabled... Profile: <b>juiceshop_dos</b>
Bot Defense Profile	Enabled... Profile: <b>Balanced_Bot_Profile</b>
Application Cloud Security Services	Disabled
DataSafe Profile	Disabled
Log Profile	Enabled... Selected: /Common Balanced_Bot_Log Log all requests local-dos Available: /Common Log illegal requests global-network local-bot-defense

Update

(../..//\_images/login\_vs.png)

### Define Login & Logout Pages¶

1. To configure a login page, go to **Security > Application Security > Sessions and Logins > Login Pages List**. Ensure the **juiceshop\_blocking** is selected at the top-middle-left of

the GUI and click **Create**.

2. We'll now populate the form with data gathered from the browser inspection tools during a login attempt as shown below.

The screenshot shows the OWASP Juice Shop application. At the top, there's a navigation bar with a logo, account information, and a shopping basket icon. Below it is a section titled "All Products" displaying four items: Apple Juice (1000ml) for 1.99, Apple Pomace for 0.89, and Banana Juice (1000ml) for 1.99. Below this is a browser's developer tools Network tab. A green arrow points to the "Response" tab, which is selected. Another green arrow points to the "Response Payload" section, where a JSON object is displayed:

```
{ "authentication": { "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dX..."}}
```

([../../../../\\_images/response.png](#))

3. Fill out the **Login Page Properties** and **Access Validation** fields as shown and then click **Create**.

The screenshot shows the Security > Application Security > Sessions and Logins > Login Pages List interface. At the top, there's a dropdown menu, a learning mode switch, and an "Apply Policy" button. The main area has two sections: "Login Page Properties" and "Access Validation". The "Login Page Properties" section contains fields for "Login URL" (set to "Explicit | HTTPS | POST | /rest/user/login"), "Authentication Type" (set to "JSON / AJAX Request"), "Username JSON Element" (set to "email"), and "Password JSON Element" (set to "password"). The "Access Validation" section contains several fields:

- "Expected validation header name and value (for example, Location header)": "token" (highlighted with a green box)
- "NOT Expected validation header name and value (for example, Location header)": (empty)
- "Expected validation domain cookie name": (empty)
- "Expected HTTP response status code": "200" (highlighted with a green box)
- "NOT Expected HTTP response status code": (empty)

([../../../../\\_images/loginp.png](#))

4. From the tab bar at the top middle of the GUI, select **Login Enforcement** and populate the form as shown below. The **/profile** URI should never have attempted access without authentication.
5. Click **Save** and make note of the **Note** in red txt. We will configure **Learning and Blocking Settings** momentarily.

Security » Application Security : Sessions and Logins : Login Enforcement

Login Pages List Logout Pages List Login Enforcement Session Tracking

Juiceshop\_blocking Learning Mode: Manual

**Login Enforcement**

Expiration Time	Disabled
Authenticated URLs (Wildcards supported) Example: /index.html	<input type="text" value="/profile"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>

Note: Although the feature is enabled, violations will not be alerted or learned. To change this, modify flags for the "Login URL bypassed" violation in the Learning and Blocking Settings screen

(../../../../\_images/le.png)

## Enable Session Tracking

1. Click the **Session Tracking** tab at the top middle of the screen and under **Session Hijacking** click the **Enabled** button. Read through the notes paying close attention to the ones in **red**.
  - For the first red note, regarding the bot profile, we are covered since DeviceID is enabled in our **Balanced\_Bot\_Profile** by default and it is applied to the VS.
  - The second is more informational and let's us know that non-browser entities will be blocked if they can not run the JS and produce a DeviceID.
  - The third is regarding **Learning and Blocking Settings** which we will configure in a moment.
2. Under **Session Tracking Configuration** Check the box for **Session Awareness** and click **Save and Apply Policy**.

Security > Application Security : Sessions and Logins : Session Tracking

<a href="#">Login Pages List</a>	<a href="#">Logout Pages List</a>	<a href="#">Login Enforcement</a>	<a href="#">Session Tracking</a>														
<input style="width: 150px; height: 20px; border: none; border-bottom: 1px solid #ccc; padding: 2px 5px; margin-right: 10px;" type="button" value="juiceshop_blocking"/> <input style="width: 20px; height: 20px; border: none; border-bottom: 1px solid #ccc; padding: 2px 5px; margin-right: 10px;" type="button" value="gear"/> <input checked="" type="checkbox"/> Learning Mode: Manual		<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Apply Policy"/>															
<b>Session Hijacking</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Detect Session Hijacking by Device ID Tracking</td> <td style="width: 85%;"> <input checked="" type="checkbox"/> Enabled            Note: Session cookies will be matched with the unique Device ID that originally received them            Note: Device-ID mode must be configured in bot profile for this option to work.            Note: Although ASM Cookie Hijacking does not block requests, using device id will block requests from clients that do not support JavaScript            Note: Although the feature is enabled, violations will not be alerted or learned. To change this, modify flags for the "ASM Cookie Hijacking" violation in the Learning and Blocking Settings screen         </td> </tr> </table>				Detect Session Hijacking by Device ID Tracking	<input checked="" type="checkbox"/> Enabled Note: Session cookies will be matched with the unique Device ID that originally received them Note: Device-ID mode must be configured in bot profile for this option to work. Note: Although ASM Cookie Hijacking does not block requests, using device id will block requests from clients that do not support JavaScript Note: Although the feature is enabled, violations will not be alerted or learned. To change this, modify flags for the "ASM Cookie Hijacking" violation in the Learning and Blocking Settings screen												
Detect Session Hijacking by Device ID Tracking	<input checked="" type="checkbox"/> Enabled Note: Session cookies will be matched with the unique Device ID that originally received them Note: Device-ID mode must be configured in bot profile for this option to work. Note: Although ASM Cookie Hijacking does not block requests, using device id will block requests from clients that do not support JavaScript Note: Although the feature is enabled, violations will not be alerted or learned. To change this, modify flags for the "ASM Cookie Hijacking" violation in the Learning and Blocking Settings screen																
<b>Session Tracking Configuration</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Session Awareness</td> <td style="width: 85%;"> <input checked="" type="checkbox"/> Enabled  <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Use All Login Pages"/> </td> </tr> <tr> <td>Application Username</td> <td>Note: Configure the login page that the system uses to detect the application's user name and associate it with the HTTP session.</td> </tr> </table>				Session Awareness	<input checked="" type="checkbox"/> Enabled <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Use All Login Pages"/>	Application Username	Note: Configure the login page that the system uses to detect the application's user name and associate it with the HTTP session.										
Session Awareness	<input checked="" type="checkbox"/> Enabled <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Use All Login Pages"/>																
Application Username	Note: Configure the login page that the system uses to detect the application's user name and associate it with the HTTP session.																
<b>Violation Detection Actions</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Track Violations and Perform Actions</td> <td style="width: 85%;"> <input checked="" type="checkbox"/> Enabled  <input type="text" value="900"/> seconds            Note: The Violation Action thresholds will track the configured number of violations by counting the number of violations within this time period. For example, a threshold might be "count 10 violation in the last 900 seconds", where the time period used is this value.         </td> </tr> </table>				Track Violations and Perform Actions	<input checked="" type="checkbox"/> Enabled <input type="text" value="900"/> seconds Note: The Violation Action thresholds will track the configured number of violations by counting the number of violations within this time period. For example, a threshold might be "count 10 violation in the last 900 seconds", where the time period used is this value.												
Track Violations and Perform Actions	<input checked="" type="checkbox"/> Enabled <input type="text" value="900"/> seconds Note: The Violation Action thresholds will track the configured number of violations by counting the number of violations within this time period. For example, a threshold might be "count 10 violation in the last 900 seconds", where the time period used is this value.																
<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Block All"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Log All Requests"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Delay Blocking"/>		<a href="#">View Session Tracking Status...</a>															
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Description</td> <td>When this action is triggered, the system blocks all requests from the user, session, device ID, or IP address, respectively. Which URLs are blocked can be configured with the "Blocked URLs" setting, to allow blocking all URLs or only the Authenticated URLs which are protected by the configured Login Page(s).</td> </tr> <tr> <td>Username Threshold</td> <td> <input type="checkbox"/> Enable <input type="text" value="20"/> violations            Note: For users which caused <b>20 violations</b> in the last <b>900 seconds</b>, the system will block all requests.         </td> </tr> <tr> <td>Session Threshold</td> <td> <input type="checkbox"/> Enable <input type="text" value="20"/> violations            Note: For HTTP sessions which caused <b>20 violations</b> in the last <b>900 seconds</b>, the system will block all requests.         </td> </tr> <tr> <td>Device ID Threshold</td> <td> <input type="checkbox"/> Enable <input type="text" value="30"/> violations            Note: For Device IDs which caused <b>30 violations</b> in the last <b>900 seconds</b>, the system will block all requests.            Note: Device-ID mode must be configured in bot profile for this option to work.         </td> </tr> <tr> <td>IP Address Threshold</td> <td> <input type="checkbox"/> Enable <input type="text" value="60"/> violations            Note: For IP addresses which caused <b>60 violations</b> in the last <b>900 seconds</b>, the system will block all requests.         </td> </tr> <tr> <td>Blocked URLs</td> <td> <input checked="" type="radio"/> Block all URLs  <input type="radio"/> Block Authenticated URLs [<a href="#">Change Login Enforcement Settings</a>]         </td> </tr> <tr> <td>Block All Period</td> <td> <input type="radio"/> Infinite <input checked="" type="radio"/> User-defined: <input type="text" value="600"/> seconds         </td> </tr> </table>				Description	When this action is triggered, the system blocks all requests from the user, session, device ID, or IP address, respectively. Which URLs are blocked can be configured with the "Blocked URLs" setting, to allow blocking all URLs or only the Authenticated URLs which are protected by the configured Login Page(s).	Username Threshold	<input type="checkbox"/> Enable <input type="text" value="20"/> violations Note: For users which caused <b>20 violations</b> in the last <b>900 seconds</b> , the system will block all requests.	Session Threshold	<input type="checkbox"/> Enable <input type="text" value="20"/> violations Note: For HTTP sessions which caused <b>20 violations</b> in the last <b>900 seconds</b> , the system will block all requests.	Device ID Threshold	<input type="checkbox"/> Enable <input type="text" value="30"/> violations Note: For Device IDs which caused <b>30 violations</b> in the last <b>900 seconds</b> , the system will block all requests. Note: Device-ID mode must be configured in bot profile for this option to work.	IP Address Threshold	<input type="checkbox"/> Enable <input type="text" value="60"/> violations Note: For IP addresses which caused <b>60 violations</b> in the last <b>900 seconds</b> , the system will block all requests.	Blocked URLs	<input checked="" type="radio"/> Block all URLs <input type="radio"/> Block Authenticated URLs [ <a href="#">Change Login Enforcement Settings</a> ]	Block All Period	<input type="radio"/> Infinite <input checked="" type="radio"/> User-defined: <input type="text" value="600"/> seconds
Description	When this action is triggered, the system blocks all requests from the user, session, device ID, or IP address, respectively. Which URLs are blocked can be configured with the "Blocked URLs" setting, to allow blocking all URLs or only the Authenticated URLs which are protected by the configured Login Page(s).																
Username Threshold	<input type="checkbox"/> Enable <input type="text" value="20"/> violations Note: For users which caused <b>20 violations</b> in the last <b>900 seconds</b> , the system will block all requests.																
Session Threshold	<input type="checkbox"/> Enable <input type="text" value="20"/> violations Note: For HTTP sessions which caused <b>20 violations</b> in the last <b>900 seconds</b> , the system will block all requests.																
Device ID Threshold	<input type="checkbox"/> Enable <input type="text" value="30"/> violations Note: For Device IDs which caused <b>30 violations</b> in the last <b>900 seconds</b> , the system will block all requests. Note: Device-ID mode must be configured in bot profile for this option to work.																
IP Address Threshold	<input type="checkbox"/> Enable <input type="text" value="60"/> violations Note: For IP addresses which caused <b>60 violations</b> in the last <b>900 seconds</b> , the system will block all requests.																
Blocked URLs	<input checked="" type="radio"/> Block all URLs <input type="radio"/> Block Authenticated URLs [ <a href="#">Change Login Enforcement Settings</a> ]																
Block All Period	<input type="radio"/> Infinite <input checked="" type="radio"/> User-defined: <input type="text" value="600"/> seconds																
<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Save"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Restore Defaults"/>																	

(../../../../\_images/session.png)

3. Navigate to **Security > Application Security > Policy Building > Learning and Blocking Settings > Sessions and Logins**

4. Check the box for **Learn, Alarm and Block** for both **ASM Cookie Hijacking** and **Login URL bypassed** and click **Save** and **Apply Policy**.

Security > Application Security : Policy Building : Learning and Blocking Settings

Traffic Learning Learning and Blocking Settings

juiceshop\_blocking  Learning Mode: Manual

**Policy Building Settings** Search in Policy Building Settings Note: Click Save to retain any changes you made on this screen.

- ▶ Antivirus
- ▶ Attack Signatures
- ▶ CSRF Protection
- ▶ Content Profiles
- ▶ Cookies
- ▶ Data Guard
- ▶ Evasion technique detected (8 out of 8 subviolations are enabled)  Learn  Alarm  Block
- ▶ File Types
- ▶ General Settings
- ▶ Headers
- ▶ HTTP protocol compliance failed (14 out of 19 subviolations are enabled)  Learn  Alarm  Block
- ▶ IP Addresses and Geolocations
- ▶ Parameters
- ▶ Redirection Domains
- ▶ Server Technologies
- ▶ Sessions and Logins  Detect login pages
 

	<input type="checkbox"/> Learn	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block	Violation
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		ASM Cookie Hijacking <input type="button"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Access from disallowed User/Session/IP/Device ID <input type="button"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Brute Force: Maximum login attempts are exceeded <input type="button"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Login URL bypassed <input type="button"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Login URL expired <input type="button"/>

(../../../../\_images/sessionaware.png)

## Test Login Enforcement¶

1. Open a new tab in Chrome Browser and paste in the following "login enforced" URL:  
<https://juiceshop.f5agility.com/profile>
2. Your attempt should be blocked:

BIG-IP® - ip-10-1-1-4.us-west-2  Request Rejected  +

← → C ⚠ Not secure | juiceshop.f5agility.com/profile

F5 Advanced W...  OWASP Juice S...  Test - OWASP J...

The requested URL was rejected. Please consult with your administrator.

Your support ID is: 17103323400677359642

[\[Go Back\]](#)

(../../../../\_images/block.png)

3. Back in Advanced WAF tab, navigate to **Security > Event Logs > Application > Requests** and locate the blocked request for **/profile**. Note the reason for the block then click on **View** under Suggestions to open a new tab to the learning suggestions screen.

The screenshot shows the 'Event Logs : Application : Requests' section of the f5agility interface. A specific entry for 'Login URL bypassed' is highlighted with a green arrow pointing to the 'View...' button in the 'Triggered Violations' panel. The 'Request Details' panel shows the following information:

Geolocation	N/A
Source IP Address	10.1.10.100:52436
Device ID	N/A
Microservice	N/A
Time	2021-03-11 10:15:50

The 'Request' panel shows the raw HTTP request details.

(../../../../\_images/blocked1.png)

4. You will notice a learning suggestion for this since we enabled learning for this violation in **Learning and Blocking Settings**.
5. Look at this suggestion very carefully. It has a score of 100% and comes from a trusted IP. The suggested action is to **Remove /profile from Authenticated URLs** which is something we definitely DO NOT want to do.
6. Learning suggestions can be tricky especially if they are coming from a trusted source and have a high confidence learning score. Always take a close look at the suggested action. For this suggestion click **Ignore** so no further suggestions are created.

The screenshot shows the 'Traffic Learning' section of the f5agility interface. A learning suggestion for 'Login URL bypassed' is highlighted with a green box around the 'Accept' and 'Ignore' buttons. A red box highlights the 'Suggested Action: Remove /profile from Authenticated URLs' message. The 'Triggered Violations' panel shows the following information:

Violation	Occurrences
Login URL bypassed	1

The 'Request Details' panel shows the following information:

Geolocation	N/A
Source IP Address	10.1.10.100:52436
Device ID	N/A
Microservice	N/A
Time	2021-03-11 10:15:50
Enforcement Action	Block
Enforced By	Application Security Policy
Violation Rating	5 (Request is most likely a threat)
Attack Types	Forceful Browsing

(../../../../\_images/learn1.png)

## Test Session Tracking¶

1. Open a new Chrome Incognito tab by typing (CTRL+SHFT+N) then open Juice Shop and login with the account you created earlier for f5student@f5agility.com

(mailto:f5student%40f5agility.com).

2. Return to the Advanced WAF and navigate to **Security > Event Logs > Application > Requests** and click on any of them except for "/socket.io". Click **All Details** to the right.

The screenshot shows the 'Event Logs : Application : Requests' page. A specific request for '[HTTPS] /assets/public/images/products/ccg\_foil.png' is selected. The 'Request Details' pane on the right displays various metadata. The 'Device ID' field (87b983d1) and the 'Username' field (f5student@f5agility.com) are both highlighted with green boxes.

(../../../../\_images/sessions.png)

3. Click the down arrow next to **Device ID** to open the Session Tracking details. Check the box to enable **Log All Requests** and click **Change**. You are now tracking all sessions from this Device ID.

The screenshot shows the 'Event Logs : Application : Requests' page with the same selected request. The 'Request Details' pane is visible. An arrow points to the 'Device ID' dropdown in the 'Session Tracking details' sub-pane. The 'Log All Requests' checkbox is checked and highlighted with a green box.

(../../../../\_images/did.png)

4. Repeat this process for the username field as well to track all sessions from **f5student**

Security > Event Logs : Application : Requests

Application Protocol Network Dos Bot Defense Logging Profiles

Order by Date Newest ▾

Requests

- [HTTPS] /assets/public/images/products/... 10.1.10.100 200 10:48:39 2021-03-11
- [HTTPS] /assets/public/images/produ... 10.1.10.100 200 10:48:39 2021-03-11
- [HTTPS] /assets/public/images/produ... 10.1.10.100 200 10:48:39 2021-03-11
- [HTTPS] /api/Quantitys/ 10.1.10.100 200 10:48:39 2021-03-11
- [HTTPS] /assets/public/images/produ... 10.1.10.100 200 10:48:39 2021-03-11
- [HTTPS] /assets/public/images/produ... 10.1.10.100 200 10:48:39 2021-03-11
- [HTTPS] /rest/basket/6 10.1.10.100 200 10:48:39 2021-03-11
- [HTTPS] /rest/user/login 10.1.10.100 200 10:48:39 2021-03-11

Delete Export

[HTTPS] /assets/public/images/products/ccg\_foil.png

Request Details

Geolocation	N/A	Enforcement Action
Source IP Address	10.1.10.100:54074	Enforced By
Device ID	87b983d1	Violation Rating
Microservice	N/A	Attack Types
Time	2021-03-11 10:48:39	Request Status
Username	f5student@f5agility.com	Blocking Exception Reason

Session Tracking details

Action Flag	State at Log Time	Current State
Log All Requests	Disabled	<input checked="" type="checkbox"/> Enabled
Delay Blocking	Disabled	<input type="checkbox"/> Enabled
Block All	Disabled	<input type="checkbox"/> Enabled

Change Release All

Support ID	17103323400677360937	Severity
Protocol Info	HTTP/1.1	Signatures CVEs

Request

(../../../../\_images/user.png)

5. Navigate to **Reporting > Application > Session Tracking Status** and review the entries that were just created from the application request event log.
6. Click “View Requests” for either of them to see all requests filtered by either the Device ID or Username. You may also use this page to release the Username or Device ID from Session Tracking.
7. These features are useful for forensic purposes as well as blocking access to applications by Device-ID, Username, etc.
8. Finally, navigate to **Security > Application Security > Sessions and Logins > Session Tracking** and review the other more detailed actions you can take based off of Devie ID, Username etc.

This concludes Lab 4