ORNL/TM-2021/2091

Protecting Websites from Cross-Site Scripting (XSS) Attacks:

A Novel Configuration using Pulse Secure© Pulse Connect Secure© and Virtual Web Application Firewall (vWAF)

B. Nance
K. O'Connor

July 2021

Approved for public release. Distribution is unlimited.

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

ORNL/TM-2021/2091

Computer Science and Mathematics Division
Performance Engineering Group

Protecting Websites from Cross-Site Scripting (XSS) Attacks: A Novel Configuration using Pulse Secure© Pulse Connect Secure© and Virtual Web Application Firewall (vWAF)

Brad Nance
Kellen O'Connor

July 2021

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ACL	Access Control List
ADC	application delivery controller
BPM	Business Process Management
CVI	Chemical-terrorism Vulnerability Information
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
PCS©	Pulse Connect Secure©
URL	Uniform Resource Locator
VPN	Virtual Private Network
vTM	Virtual Traffic Manager (Pulse Secure©)
vWAF	Virtual Web Application Firewall (Pulse Secure©)
WAF	web application firewall
XSS	Cross-Site Scripting

ABSTRACT

Cross-site scripting (XSS) is an attack that leverages the ability of a malicious actor to submit data or commands through user input forms or through client-side manipulation of the Uniform Resource Locator. Web application firewalls (WAFs) are a first line of defense where common Uniform Resource Locator (URL) patterns are analyzed to detect and block known attacks.

This paper describes a novel configuration using the Pulse Secure© Pulse Connect Secure© (PCS©) Secure Socket Layer Virtual Private Network software and Pulse Secure© Virtual Web Application Firewall (vWAF) that protects a website from XSS attacks. This paper also presents novel aspects of the configuration that control the redirection of traffic through the vWAF and provide fine-grained behavioral control at the application level while decoupling the PCS and vWAF configurations. The intended audience for this paper comprises system and site administrators who are familiar with standard web server environments. These configuration details might prove useful during the design of a more secure infrastructure.

1. INTRODUCTION

Cross-site scripting (XSS), one of the most prevalent forms of client-side attacks, is when bad actors attempt to access sensitive information from the backend web server and other systems on the backend network. Some XSS attacks attempt to access client-side sensitive information, such as cookies. Web application firewalls (WAFs) are a first line of defense where common Uniform Resource Locator (URL) patterns are analyzed to detect and block known attacks.

This paper describes a novel configuration using the Pulse Secure© Pulse Connect Secure© (PCS©) Secure Socket Layer Virtual Private Network software and Virtual Web Application Firewall (vWAF) that protects a website from XSS attacks. This paper also presents novel aspects of the configuration that control the redirection of traffic through the vWAF and provide fine-grained behavioral control at the application level while decoupling the PCS and vWAF configurations. The intended audience for this paper comprises system and site administrators who are familiar with standard web server environments. These configuration details might prove useful during the design of a more secure infrastructure.

2. CROSS-SITE SCRIPTING ATTACKS

2.1 CROSS-SITE SCRIPTING ATTACKS

XSS is an attack that leverages the ability of a malicious actor to submit data or commands through user input forms or through client-side manipulation of the URL. These attacks can cause temporary or long-term effects and can retrieve sensitive data from any targeted backend system or victim's browser.

2.2 EXAMPLE OF AN XSS ATTACK

Figure 1 shows the typical flow of an XSS attack using a site that allows a user to submit a product review, as follows:

1. A malicious actor submits a script as a review, which gets loaded into the website database.
2. A victim accesses the review.
3. The malicious script is executed on the victim's browser.
4. The cookie information is sent to the attacker containing information that allows the attacker to impersonate the victim.

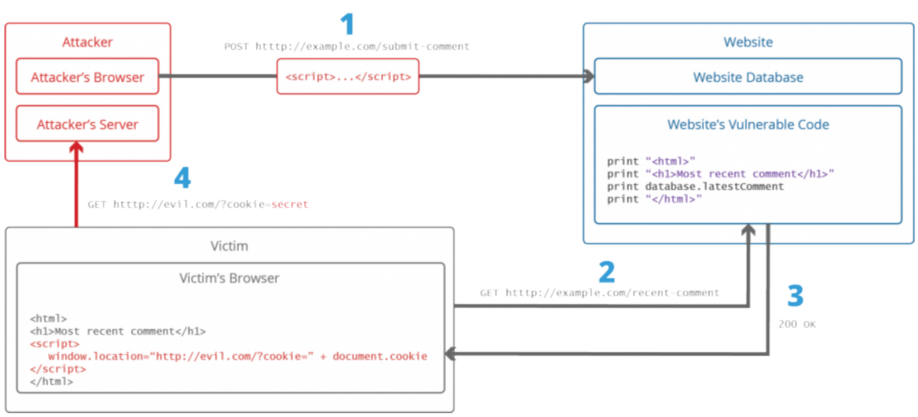

Figure 1. Example of XSS attack execution.

3. WEB APPLICATION FIREWALLS

A WAF is a filter or shield that is applied in front of a web application that uses rules to determine if the examined hypertext transfer protocol traffic (i.e., network traffic) is safe or allowable. A WAF can be integrated with the application, or it can be a standalone hardware device dedicated to evaluating traffic. Figure 2 shows the role of a WAF in managing traffic where it is configured to block XSS attempts by malicious actors.

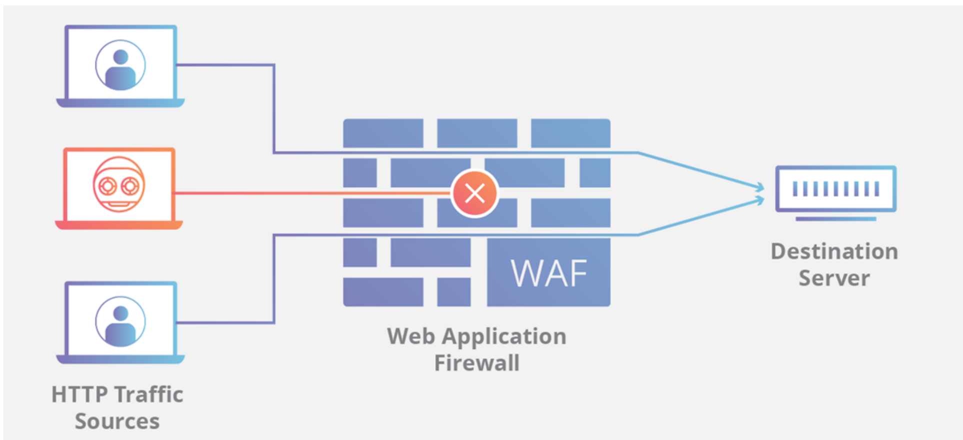

Figure 2. WAF traffic management.

4. PULSE CONNECT SECURE

PCS is a platform that runs on Pulse Secure's Secure Socket Layer Virtual Private Network software appliance and provides the following features and capabilities:

- Provides sign-in URLs.
- Provides authentication and user realm configurations.
- Provides behavior based upon host request header.
- Assigns Web Access Control Lists (ACLs) to enable access to backend web server resources. PCS operates with an implicit deny. Only requests to resources that are explicitly defined in the ACLs are allowed.

5. PULSE SECURE VIRTUAL TRAFFIC MANAGER

Pulse Secure Virtual Traffic Manager (vTM) is an application delivery controller (ADC) that provides the following functionality:

- Acts as a load balancer that allows distribution of the work across multiple nodes. Examples are round robin (i.e., rotate through all available nodes), geography, and current load.
- Forwards traffic to nodes based upon traffic control rules, like session persistence and load balancing.
- Includes the vWAF as a software layer added on top of the vTM with an integrated graphical user interface.

- Analyzes traffic using a complex set of regular expression rules. For example, the following regular expression would be used to detect an attempted execution of common shell commands.

  (?:(`|\||;|&|\$\())\s*((c|k|ba)?sh|chmod|dir|chown|env|export|ftp|pwd|nc|ls|id|cat|gcc|g\+\+|perl|pagefile|python|ruby|netstat|ps|uname|echo|ping)(`|\||;|\s|\)|\$)

- Unlike PCS, the vTM operates with an implicit allow. Only traffic that meets the explicit criteria is blocked.
- Can utilize a different set of rules for each application based upon the value of the host request header.

Figure 3 shows how the Pulse Secure vTM integrates with the application architecture.

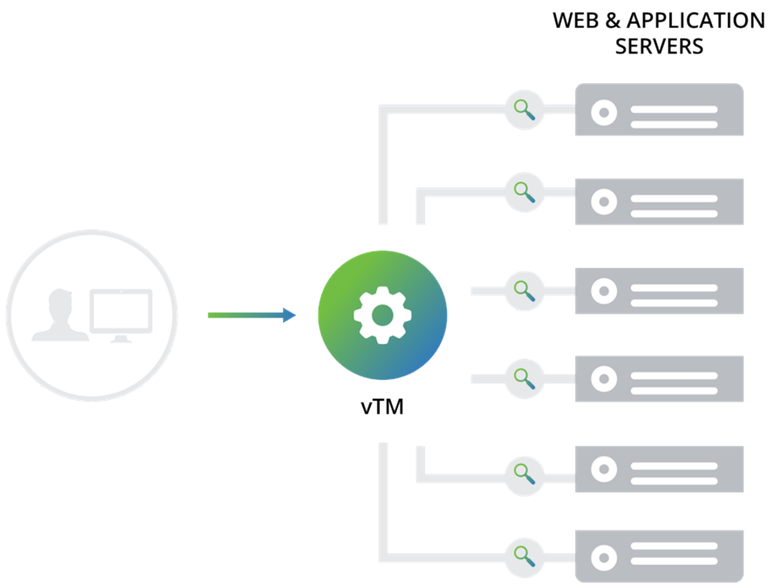

Figure 3. Pulse Secure Virtual Traffic Manager (vTM).

6. UNPROTECTED CONFIGURATION

This section discusses the unprotected configuration to delineate more clearly the differences between the unprotected configuration and the protected configuration. The unprotected configuration does not utilize a WAF and is potentially vulnerable to XSS attacks. This configuration includes the following four elements that are discussed in this section.

1. Application – Fully Qualified Domain Name (FQDN) Associations
2. Domain Name System (DNS) Configuration
3. PCS Access Flow
4. PCS Request Flow

6.1 UNPROTECTED APPLICATION – FQDN ASSOCIATIONS

Table 1 shows the five unique FQDNs that correspond to the application servers. Since fine-grained control at the application level is not needed, application-specific FQDNs are not used.

Table 1. Application – FQDN Associations

Application	FQDN
Chemical Industry User Registration	regweb.ornl.gov
Chemical Industry Portal and Applications	collweb.ornl.gov
Chemical Industry Password Reset	regweb.ornl.gov
Chemical-terrorism Vulnerability Information (CVI) Training	regweb.ornl.gov
CVI User Management	regweb.ornl.gov
Personnel Surety Application	psweb.ornl.gov
Chemical Security Operations Portal and Applications	rptweb.ornl.gov
Chemical Security Operations Password Reset	rptweb.ornl.gov
Knowledge Center	rptweb.ornl.gov
Business Process Management (BPM) Application	bpmweb.ornl.gov

6.2 UNPROTECTED DNS CONFIGURATION

Table 2 shows the list of DNS records and values associated with each FQDN. Only Authoritative (A) DNS records are needed for each of the FQDNs because a WAF is not part of this configuration and detailed control of each application hosted on the servers is not necessary.

Table 2. FQDN Record Types and Values

FQDN	Record Type	Value
collweb.ornl.gov	A	<IP address>
regweb.ornl.gov	A	<IP address>
psweb.ornl.gov	A	<IP address>
rptweb.ornl.gov	A	<IP address>
bpmweb.ornl.gov	A	<IP address>

6.3 UNPROTECTED PCS ACCESS FLOW

Figure 4 shows the access flow for the unprotected configuration where the user is directed to the application server from PCS.

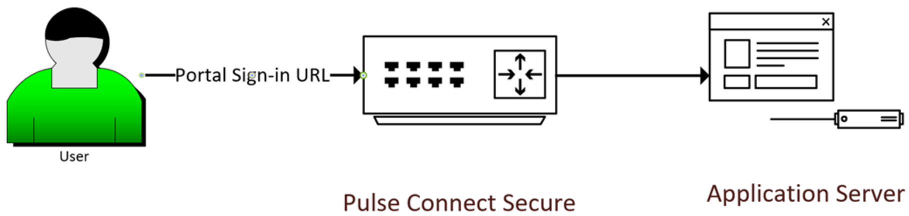

Figure 4. Unprotected PCS access flow.

6.4 UNPROTECTED PCS REQUEST FLOW

Figure 5 shows the flow for an application request for the unprotected configuration. Web ACLs are granted based upon the user role associated with the application request. If the ACL for the request resource has been assigned, the access is allowed; otherwise, access is denied.

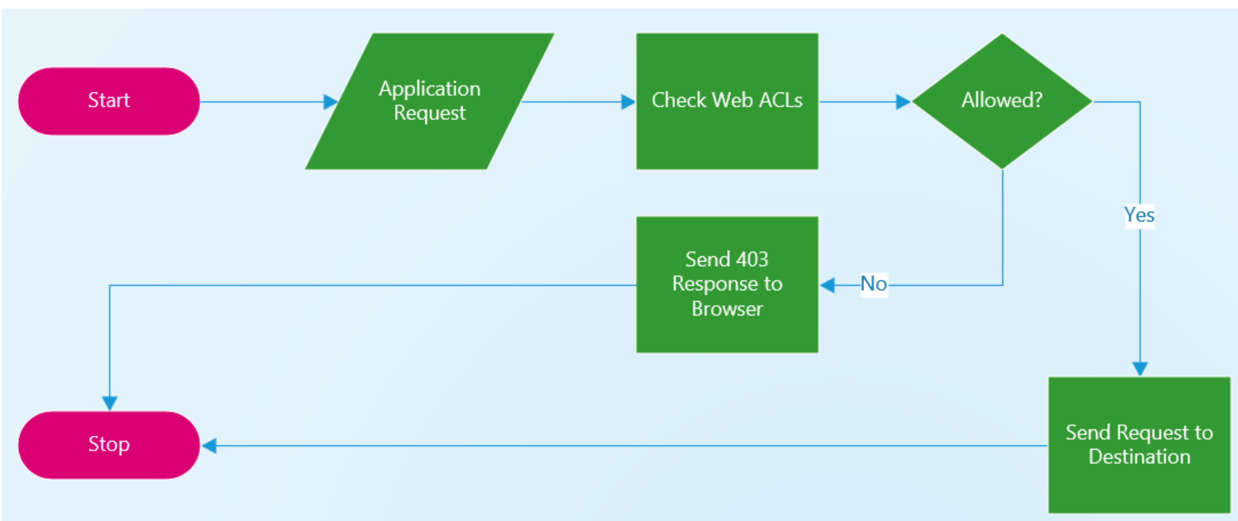

Figure 5. Unprotected PCS request process.

7. PROTECTED CONFIGURATION

The protected configuration incorporates a WAF and implements fine-grained control at the application level. The following five elements of this configuration listed are discussed in this section.

1. Application – FQDN Associations
2. DNS Configuration
3. Redirection of Traffic through vWAF

4. Pulse Secure vWAF Access Flow
5. Pulse Secure vWAF Request Flow

7.1 PROTECTED APPLICATION – FQDN ASSOCIATIONS

For the protected configuration, each application is assigned a unique FQDN so that fine-grained control at the application level is possible. The following unique vWAF attributes are configured for each application:

- Application paths
- Rulesets
- Error detection behavior

Application paths are part of the URL. If the path of the URL matches an application path defined on the vWAF, then the ruleset is evaluated.

Rulesets are collections of regular expressions that are tested for a match with known XSS attacks. If the URL matches an element of the ruleset, then the error detection behavior is triggered, ensuring that the URL does match a known XSS attack.

Error detection behavior is determined by the mode, detection or protection, and configuration of the vWAF. If the vWAF is in detection mode, then the error is simply logged. If the vWAF is in protection mode, then, based upon the configuration, the vWAF either redirects the user to a specified page or returns a 403 forbidden error code along with a custom web page.

Table 3 shows the FQDNs that enable fine-grained control at the application level.

Table 3. Protected Application – FQDN Associations

Application	FQDN
Chemical Industry User Registration	regweb.ornl.gov
Chemical Industry Portal and Applications	collweb.ornl.gov
Chemical Industry Password Reset	csatfpweb.ornl.gov
Chemical-terrorism Vulnerability Information (CVI) Training	cviweb.ornl.gov
CVI User Management	cviumweb.ornl.gov
Personnel Surety Application	psweb.ornl.gov
Chemical Security Operations Portal and Applications	rptweb.ornl.gov
Chemical Security Operations Password Reset	csfpweb.ornl.gov
Knowledge Center	kcweb.ornl.gov
Business Process Management (BPM) Application	bpmweb.ornl.gov

7.2 PROTECTED DNS CONFIGURATION

For the protected configuration, Alias (CNAME) DNS records are used because vWAF behavior is host request header based. Table 4 shows the record types and values associated with the FQDNs. The bold entries indicate an application FQDN that is an alias to an authoritative host. For example, csatfpweb, cviweb, and cviumweb are aliases for the authoritative host regweb.

Table 4. Protected DNS Configurations

FQDN	Record Type	Value
regweb.ornl.gov	A	<IP address>
csatfpweb.ornl.gov	**CNAME**	**regweb.ornl.gov**
cviweb.ornl.gov	**CNAME**	**regweb.ornl.gov**
cviumweb.ornl.gov	**CNAME**	**regweb.ornl.gov**
collweb.ornl.gov	A	<IP address>
psweb.ornl.gov	A	<IP address>
rptweb.ornl.gov	A	<IP address>
csfpweb.ornl.gov	**CNAME**	**rptweb.ornl.gov**
kcweb.ornl.gov	**CNAME**	**rptweb.ornl.gov**
bpmweb.ornl.gov	A	<IP address>

7.3 PROTECTED REDIRECTION OF TRAFFIC THROUGH VWAF

For websites to be protected, application requests must be redirected to the vWAF. This redirection is accomplished by adding local host entries to the PCS configuration so that the FQDNs resolve to the Internet Protocol address of the vWAF. This local host approach provides greater flexibility for testing and debugging because the vWAF can be "turned off" simply by removing the entry for an application FQDN without making any additional changes to the PCS configuration. It also allows non-web traffic, like Secure Shell Protocol, or internal testing, to be routed directly to the correct servers. Figure 6 shows the local host entries in the PCS configuration that redirect traffic to the vWAF.

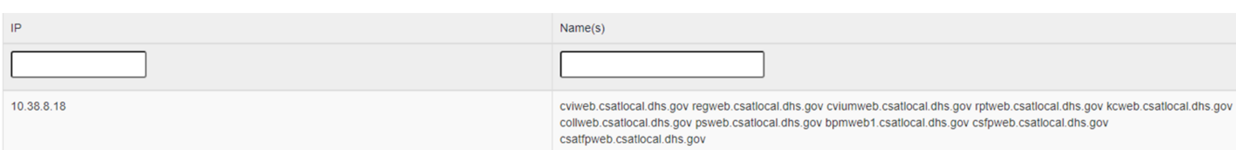

Figure 6. Local host entries in PCS configuration.

7.4 PROTECTED VWAF ACCESS FLOW

Figure 7 shows the access flow for the protected configuration where traffic from PCS is redirected to the vWAF for processing.

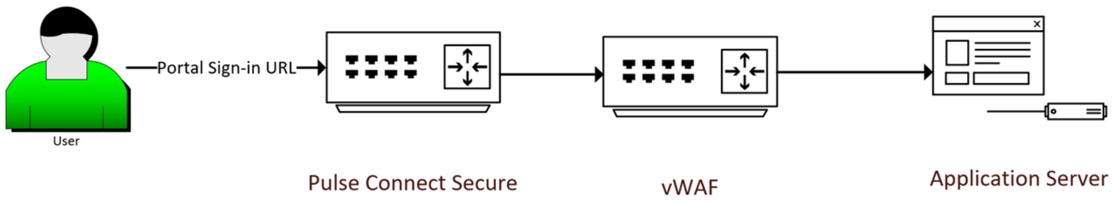

Figure 7. Protected vWAF access flow.

7.5 PROTECTED VWAF REQUEST FLOW

Figure 8 shows the flow for an application request for the protected configuration. The initial flow is identical to the unprotected configuration until after the Web ACLs are checked. If a Web ACL exists for the requested resource, the next step is to check for a local host entry for the application FQDN. If that exists, the request is forwarded to the vWAF where the application path and associated rulesets are checked for a match. If a match is found, the configured error behavior is executed.

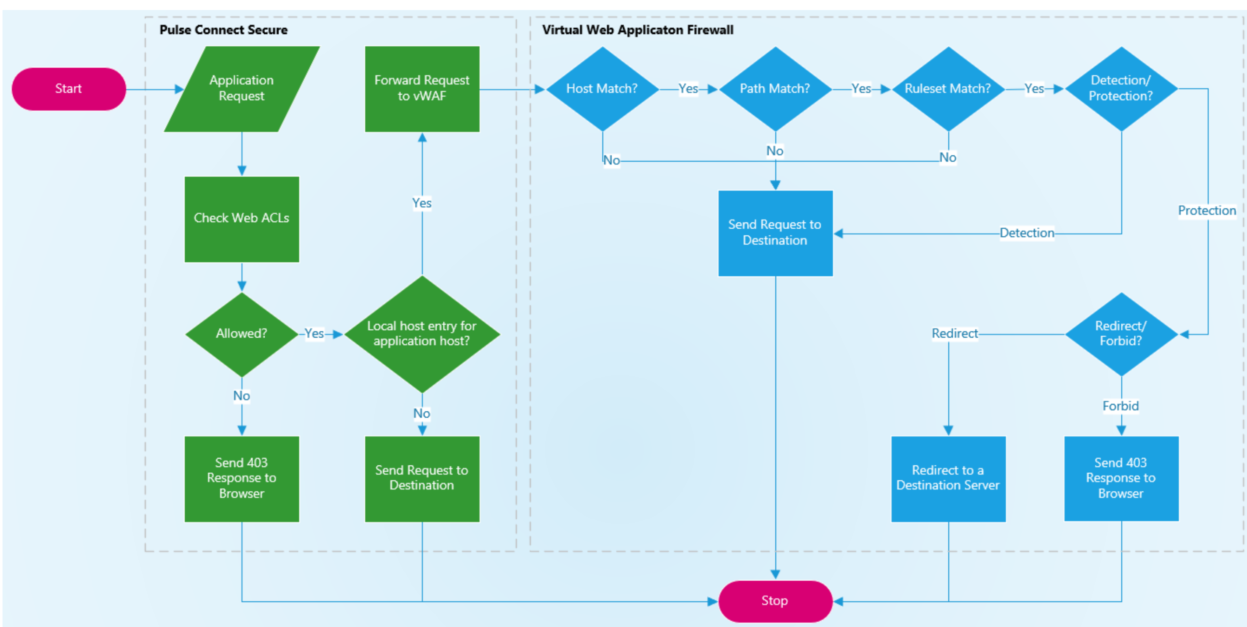

Figure 8. Protected vWAF request flow.

7.6 APPLICATION–LEVEL CONTROL

Application-level control is accomplished by assigning a unique FQDN to each application and is possible because vWAF behavior is based upon the host request header of the corresponding application. Table 5 shows the unique FQDN for each application, along with other vWAF configuration attributes.

Table 5. Application-Level Control Elements

Application	Authenticated?	Application Server	Host FQDN	vWAF Mode	Error Behavior (when protected)
Chemical Industry User Registration	No	regweb	regweb.ornl.gov	Protection	Redirect
Chemical Industry Portal and Applications	Yes	collweb	collweb.ornl.gov	Detection	Forbid
Chemical Industry Password Reset	No	regweb	csatfpweb.ornl.gov	Protection	Redirect
Chemical-terrorism Vulnerability Information (CVI) Training	No	regweb	cviweb.ornl.gov	Protection	Redirect
CVI User Management	Yes	regweb	cviumweb.ornl.gov	Detection	Forbid
Personnel Surety Application	Yes	psweb	psweb.ornl.gov	Detection	Forbid
Chemical Security Operations Portal and Applications	Yes	rptweb	rptweb.ornl.gov	Detection	Forbid
Chemical Security Operations Password Reset	No	rptweb	csfpweb.ornl.gov	Protection	Redirect
Knowledge Center	No	rptweb	kcweb.ornl.gov	Protection	Redirect
Business Process Management (BPM) Application	Yes	bpmweb	bpmweb.ornl.gov	Detection	Forbid

8. CONCLUSION

The integrated solution using Pulse Secure PCS and vWAF meets all established goals, as follows:

- The built-in features of the vWAF allow websites to be protected from known XSS attacks.
- The application-specific FQDNs that are DNS aliases of the underlying application servers allow fine-grained control at the application level.
- The local host configuration capabilities of PCS allow the following:
  - Control of the redirection of traffic through the vWAF.
  - Decoupling of the PCS and vWAF configurations.