FORTRA

DATASHEET (Digital Defense)

Frontline WAS™

Audit the Security of Your Web Applications with Frontline WAS™

It's an appy world and you're leading the charge. But how secure are your applications?

Web applications with their access, and transactions they process, are prime targets for criminal attackers.

Rapid web application technology changes require organizations to constantly stay abreast of new standards and best practices. With the introduction of each new web technology and the sheer volume of web based attacks, one fact remains true – securing the application(s) is non-negotiable.

				🕸 🕂 New 🛔 Account Adm
ustom :: WebAppGro	up			C Rescer •
Web Applications	Q Detah Va	dreubliss		
C http://172.20.71.96/hackadem c http://172.20.71.96/hackadem http://172.20.71.96/hackadem http://172.20.71.96/dvamDW	ic!	ts OWASP Counts	Vuln Counts	Scan Rating C ors. Ltd
D http:///22.20.71.50.6WAPP-6 http:///22.20.71.50.6WAPP-6				Web apps Vulnerabilities 3
http://172.20.71.90.01				Completed 10 Feb 20
A http://172.20.71.90.01				Time to complete
				Scan definition W
	OWIASP Top 10 B	Breakdown		
	OWIASP Top 10 B A1 Injection	Breakdown		
	A1. Injection	Breakdown relication and Session Management		
	A1. Injection	nfication and Session Management		
	A1: Injection A2: Broken Auther	ntication and Session Management ripting (XSS)		
	A1 Injection A2 Broken Auther A3 Cross-Site Scr	ntication and Session Management ripting (XSS) is Control		
	A1: Injection A2: Broken Auther A3: Cross-Site Sci A4: Broken Access	nfication and Bession Management inpling 0058) w Control onfiguration		

Quick. Comprehensive. Accurate.

Frontline Advanced[™]

Frontline Advanced is Digital Defense's flagship vulnerability management subscription offering.

Powerful and effective, Frontline Advanced is conveniently bundled into a rich, affordable, and easy to consume annual subscription that includes:

- Frontline VM scanning and features
- Unlimited users
- Client Advocate support
- Quarterly/monthly/unlimited scan frequency
- 24/7 support
- Access to Active View Dashboard
- User-friendly, aggregated scan results
- Robust filtering and labeling capabilities
- Patented host correlation

Frontline Pro[™]

Frontline Pro provides the same industry leading solution subscription as Frontline Advanced, but adds a Personal Security Analyst (PSA). PSAs perform the work of running your scans, analyzing the results, generating reports, and providing direct remediation planning guidance for you, as opposed to your security team doing that themselves. It's the ultimate outsource for all size organizations and is especially helpful for organizations that have limited security management time or expertise.

Results Are Key

At Digital Defense, we know the importance of optimizing time and resources to ensure your information security program is performing at the highest level.

Frontline WAS has been developed to provide the highest level of results through a system that is easily deployed and maintained. Enjoy the benefits of a technology you can trust to deliver unparalleled accuracy with minimal consumption of resources. Frontline WAS provides:

- High level dashboards at the scan level and a per web application to easily expose overall security postures at various levels
- Tracking of and trending on new, recurred, fixed vulnerabilities
- Frontline Security GPA[®] trending that offers a dynamic view of your security posture
- Detailed reporting to address OWASP Top 10
- Ability to compare Frontline VM and WAS Assets Ratings automatically, with no manual intervention required
-and more!

Let Us Help Identify Your Weaknesses

Contact us: <u>sales@digitaldefense.com</u> For more information visit: <u>www.DigitalDefense.com</u>

ttp://172.20.71.98/bricks/index.php :: OWASP Bricks				C Re	C Rescen - D Build rep				sport	
Scan overview			Details M	verabilities Notas Associated Assuts	(a	. 5	ears)		т.	0.
http://172.20.71.986/rd	kalindex.php . OWAS	-	wine No #172	20 71 958vidustrom 6						
D P Bricks http://122.20.71.90.6vid	and	0.01	twing hepping	2011 Solenoiskope s						
	concises help	0	Add comment 4	Add label More options -			0 0	roup by	ville	rab-l
		0	Severity	Wulmerability				60	Dy 541	vert
Pages	٩	0	нон	Cosmolite Station Full: Anduction Enducing						
bricks	(1)		_	Web Server Bied SQL Injection						
• 🖿 logn-ő	T	0	HIGH	Path: Anskalope-Gridocyty			1.0			
Haccess			-	Web Server Uses Unenchoted Plaintext Form Password Fields						
📓 index.php	200	0	🕒 LOW	Path: Mtp. 2172 20 71 90 brides legis-57						
• Im login-4			-	Web Server Uses Unencrypted Plaintext Form Password Fields						
htaccoss		0	C LOW	Path: http://172.20.71.95/bricks/login-5/index.php						
🐚 index php	1000		_	2 Web Server Uses Userscrypted Planted Form Passecod Fields						
• Imagin-2 Nacessa	11	0	C LOW	Path: Anidu/topin-Srindoc.php						
index php			-	Password Form Submission Without Autocomplete noff						
· login-1		0	mo	Path; http://172.20.71.90.becks/tope-5/						
Marcona		100	-	Password Form Submission Without Autocomplete noff						
hindex php		0	INFO	Path: http://172.20.71.95/bricks/login-5/index.php						
bricks hand										
* images				Returned 7 entries				25	50	- 5
htaccess										
content-pages html										
index.php										
about Heni										
* config										
setup php										
Maccess	- C									

Inclusion and and day							
ittp://172.20.71.98	/bricks/index.ph	p :: OWA	SP Bricks			C Recon -	B Build rep
Scan overview		Details	Vulnerabilities 0	ictes Associated A	neb	Q Sea	th T- 6
	ncksindex.php OWA3	Showing 3	p.//172.20.71.96/bricks/og	mő			
D P bicks http://72.20.71.966	ricksledex.php	E Add comm	nt 🗣 Addiabes Ma	ra optiona -			Group by vulneral
		G Severity	Vulserabilit				+ Sonty Seve
Pages	a,			Re Scrieting, subagin Mindex che		+ 0	
• In bricks	(1) h		1000.000	anogo siniota php			
• 🖿 login ő	T	Detail	Data Request	Response Commente	Labris		
htpososs	THE R. L.	No. do a construction	ity Details				
■ index.php •■ login-4		A cross-	te scripting vulnerability ha		web application. Cross-site scripting occurs wh y sanitized by the web application.	en an attacker can inject arbitrary JavaScript?/T	
htsccess		There at	two different variations of	cross-site scripting called r	effective and stored. Reflective cross-site script	ing typically refers to cases where an attacker m	unt trick a user in
index php	10002					loaded. With stored cross-site scripting, an attac	
■ login-2	100					centario where this occurs is on a bulletin board- ive tricking a user into following a link that may a	
Maccesa			inclead, the user is affected			and the galaxy and the second s	
index php		Impact					
• lagin-1	1000		kar finds one of these vulti or potentially hijack a user?		e web apprearies, it may be possible to steak a	ser session tokens, make the website appear as	though it has be
Maccass		Solution					
💼 index.php			ecific upgrades may be av	alable to remedy this issue	Please consult the web server software vend	for for additional information.	
bricks.html							1000
• Imagos	1000					the code that handles the vulnerable parameters effectively prevents characters that are used in	
Maccess						somal References section for other specific rame	
content-pages html	100						Co to definit
index php							- 00-10 00178
about html				nier Blind SQL Injection		1.0	
 config 		-	Path, Brikk	wlogin-Sindex.php		1.0	
who php		-	E the Se	ner Uses Unencrypted/Ple	output Known Classroom Kindda		
		C 0 10		(172.20.71.90b-skafoge-		5 0	

About Fortra



Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at <u>fortra.com</u>.