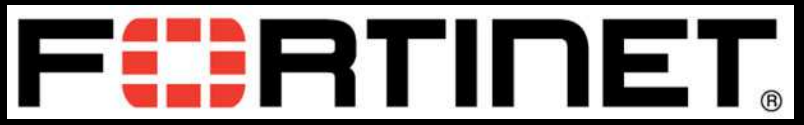
App2Own Bug Bounty contest statistics and winners

November 19th, 2015

DefCamp 2015

Cristian Patachia, Orange

Madalin Vasile, Fortinet



why are we doing this
looking to increase awareness

Orange promotes Bug Bounty initiatives in order to test and improve the accuracy of its cybersecurity solutions developed to protect the Internet access for companies.

Orange is the first telecommunication operator from Romania that supports vulnerabilities identification and responsible disclosure.

main points to follow
for a winning competition

- start : November 1st
- register
- info about the target
- bypass the security to reach the target
- send asap the exploit report
- if validated the rank will be updated
- stop : November 14th

rules of game
for a responsible disclosure

- points based on the vulnerability risk you managed to exploit
- play only as an individual, the rule of first to report the same bypass
- dashboard page with assets you have permission to attack
- cheating or destroying challenges is not allowed
- (D)DOS is not accepted
- trying to ignore the rules above will get you banned
- innovative methods will get you extra points

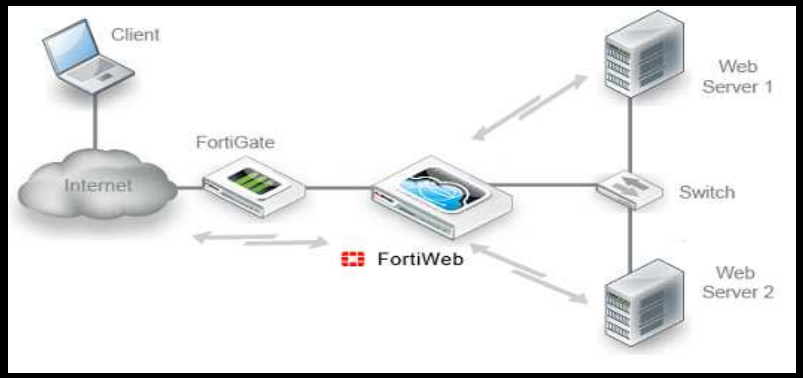
infrastructure set-up
to emulate real life situation

Target Web Server

FortiGate 500D [v5.2.3, build670]

FortiWeb 400C [v5.37,build0478 150618]

FortiAnalyzer VM [v5.2.4, build0738 150923]



System Information

HA Status	
Host Name	
Serial Number	
Operation Mode	
System Time	
Firmware Version	
System Configuration	
Current Administrator	
Uptime	
Virtual Domain	

System Information

Host Name
Serial Number
Operation Mode
HA Status
System Time
Firmware Version
System Uptime
Administrative Domain
FIPS-CC Mode

System Information

Host Name	FAZVM64 [Change]
Serial Number	FAZ-VM0000048729
Platform Type	FAZVM64
System Time	Fri Nov 13 11:30:56 EET 2015 [Change]
Firmware Version	v5.2.4-build0738 150923 (GA) [Update]
System Configuration	Last Backup:N/A [Backup] [Restore]
Current Administrators	admin [Change Password] /1 in Total [Detail]
Up Time	14 days 20 hours 50 minutes 10 seconds
Administrative Domain	Enabled [Disable]
Operation Mode	Analyzer [Change]

security features activated
to emulate real life situation

FortiGate

- Antivirus
- Application Control
- Web Filtering
- IPS

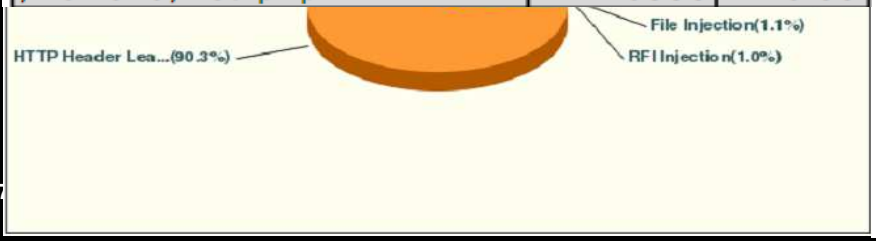
FortiWeb

- default signatures
- no fine tunning, no XML protection
- no http protocol validation, no parameter validation

detected attacks
FortiWeb

Top Attack URLs

URL	Events	Percent
/kemana/index.php	266258	25.59
/kemana/search.php	87641	8.42
/blog/wp-admin/admin.php	76404	7.34
/kemana/msg.php	61542	5.92
/blog/	49179	4.73
/xrms/xrms/login.php	37957	3.65
/xrms/xrms/login-2.php	36207	3.48
/kemana/task.php	28401	2.73
/blog/wp-admin/admin-ajax.php	26079	2.51
/kemana/public/image/exploit.php	23093	2.22
/glpi/glpi/front/login.php	13060	1.26
/kemana/list.php	10338	0.99



Top Attack Typ			
Month	Atta		
2015-nov	HTTI Leak		
	SQL (Ext		
	Bad		
	Dire		
	File		
	RFI		
	Dire		
	Cros		
	SQL		
	SSI		
	Appl Avai		
	HTTI Split		
	LFI injection	1382	0.13
	Command Injection	621	0.06
	SQL Errors leakage	556	0.05
	Path Disclosure Vulnerability by a direct request url.	288	0.03
	PHP Source Code Leakage	272	0.03
	Header Length Exceeded	178	0.02
	Cross Site Scripting (Extended)	176	0.02

Top Attack Sources

Source	Events	Percent
178.138.135.93	263597	25.34%
79.112.65.173	113824	10.94%
141.85.0.115	76702	7.37%
79.112.108.50	73006	7.02%
79.112.67.18	64472	6.20%
195.212.29.167	57387	5.52%
79.112.2.209	47221	4.54%
95.76.230.11	27636	2.66%
46.62.147.202	25394	2.44%
46.62.183.30	24259	2.33%

detected attacks
FortiGate

High Risk Applications

#	Risk	Applicati
1	Evasive	Rss

Top Applications Running Ov

#	Application
1	HTTP
2	SSL
3	File.Upload.HTTP
4	Rss
5	Silverlight
6	Atom.Publishing.Protocol
7	Httrack
8	HTTP.Segmented.Download
9	HTTP.Download.Accelerator
10	Wget.Like
11	Proxy.HTTP
12	HTTPS.BROWSER
13	HTTPS
14	Android
15	Facebook

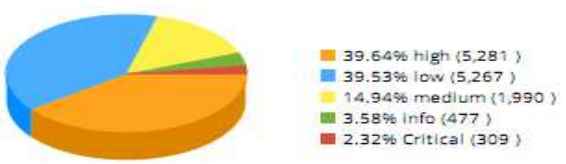
Top Viruses By Name

#	Virus Name	Occurrences
1	PHP/C99shell.BGT!tr	21
2	W32/PHPShell.A!tr	10
3	PHP/WebShell.NAF!tr	7
4	EICAR_TEST_FILE	5
5	PHP/Rst.CO!tr.bdr	3
6	PHP/C99Shell.AMB!tr.bdr	2
7	JS/Agent.KD!tr.bdr	1

Top Threats Crossing The Network

By individually reviewing both the applications and traffic flows crossing the network, threat vector identification and prevention becomes easier. Threat prevention technologies filter the total number of applications and traffic crossing the network down to those applications or packets that pose a potential risk, picking up threat vectors such as spyware, application vulnerabilities or viruses. The result is improved overall network performance and lower network latency.

Top Threat Crossing The Network



Top Critical Threats Crossing The Network

#	Attack Name	Reference	Total Num
1	Bash.Function.Definitions.Remote.Code.Execution	http://www.fortinet.com/ids/VID39294	180
2	Cisco.IOS.HTTP.Command.Execution	http://www.fortinet.com/ids/VID12188	93
3	MS.IIS.WebHits.Authentication.Bypass	http://www.fortinet.com/ids/VID15549	28
4	VxWorks.WDB.Agent.Debug.Service.Code.Execution	http://www.fortinet.com/ids/VID25633	3
5	Cisco.Command.Execution	http://www.fortinet.com/ids/VID12577	2
6	Bsguest.RemoteCommandExecution	http://www.fortinet.com/ids/VID12461	1
7	Bslist.RemoteCommandExecution	http://www.fortinet.com/ids/VID13074	1
8	OpenSSL.Heartbleed.Attack	http://www.fortinet.com/ids/VID38315	1

Top High Threats Crossing The Network

	Total Num
m/ids/VID15621	2,697
m/ids/VID15463	1,969
m/ids/VID31752	168
m/ids/VID32416	82
m/ids/VID34983	49
m/ids/VID15617	48
m/ids/VID12015	41
m/ids/VID12662	35
m/ids/VID40483	32
m/ids/VID10181	25

contest statistics
confirming Pareto principle

- 95 registered people
- 15 participants scored
- 112 received reports
- 71 validated reports
- 11,995 total points

vulnerability type	base points
SQL Injection	300
Cross Site Scripting	200
Shell Upload	350
Cross Site Request Forgery	100
Insecure Direct Object Reference	250
Full Path Disclosure	50
Local File Inclusion	200
Remote Code Execution	400
Malware Upload	50

international audience
and local sessions distribution

	Country	Sessions	% Sessions
1.	Romania	1,106	92.01%
2.	Germany	21	1.75%
3.	United Kingdom	20	1.66%
4.	United States	13	1.08%
5.	Morocco	5	0.42%
6.	Netherlands	5	0.42%
7.	Czech Republic	4	0.33%
8.	India	4	0.33%
9.	(not set)	4	0.33%
10.	Italy	3	0.25%

1.	Bucharest	**778** (70.34%)
2.	Timis County	**77** (6.96%)
3.	Bihor County	**55** (4.97%)
4.	Iasi County	**45** (4.07%)
5.	Cluj County	**43** (3.89%)
6.	Suceava County	**27** (2.44%)
7.	Dolj County	**13** (1.18%)
8.	Arges County	**11** (0.99%)
9.	Hunedoara County	**9** (0.81%)
10.	Caras-Severin County	**8** (0.72%)

Wall of Fame
and ranking

position	name	points
1.	Ionut Cernica	3500
2.	Catalin Irimie	3235
3.	Dan Poberezhnicenco	1720

Congratulations for all successful bypass attempts !!!

12.	Dragos Fedorovici	60
13.	Andrei Ghiciac	50
14.	Hertz	50
15.	Mihai Cvasnievschi	10

Thanks.
We are here for you.
We're listening.

orange™