LIETUVOS RESPUBLIKOS
VYRIAUSIOJI RINKIMŲ KOMISIJA

DEFENSE OF WEBSITES

DARIUS POVILAITIS

- Work in the cybersecurity area
- Investigations in the cybersecurity area (http://tyrimai.esec.lt / darius@esec.lt)

PRESENTAION

This presentation is a practical approach towards website defense - in particular for websites related to finance (e.g. electronic banking websites) and for websites containing massive amounts of personal data (e.g. eshop).

PRESENTAION

P.S.:

During presentation the essential information is highlighted in yellow or red

If you have any question please do ask instantly

MAIN REASONS FOR INTRUSIONS

- money
- information
- discreditation
- illegal usage of resources – e.g. cryptomining
- etc.

WHY SYSTEMS ARE INSECURE?

- Vulnerabilities in the systems are due to many different factors – we will not analyze reasons for that. The main question is - how to prevent or reduce impact of those possible vulnerabilities ?
- While designing the system you should consider security issues from very beginning. Such an approach for system design from the security point of view is given in
- „OWASP Testing Guide“. Together with a “owasp programming guide” they for strong basis for system security.

IMPORTANT !!!

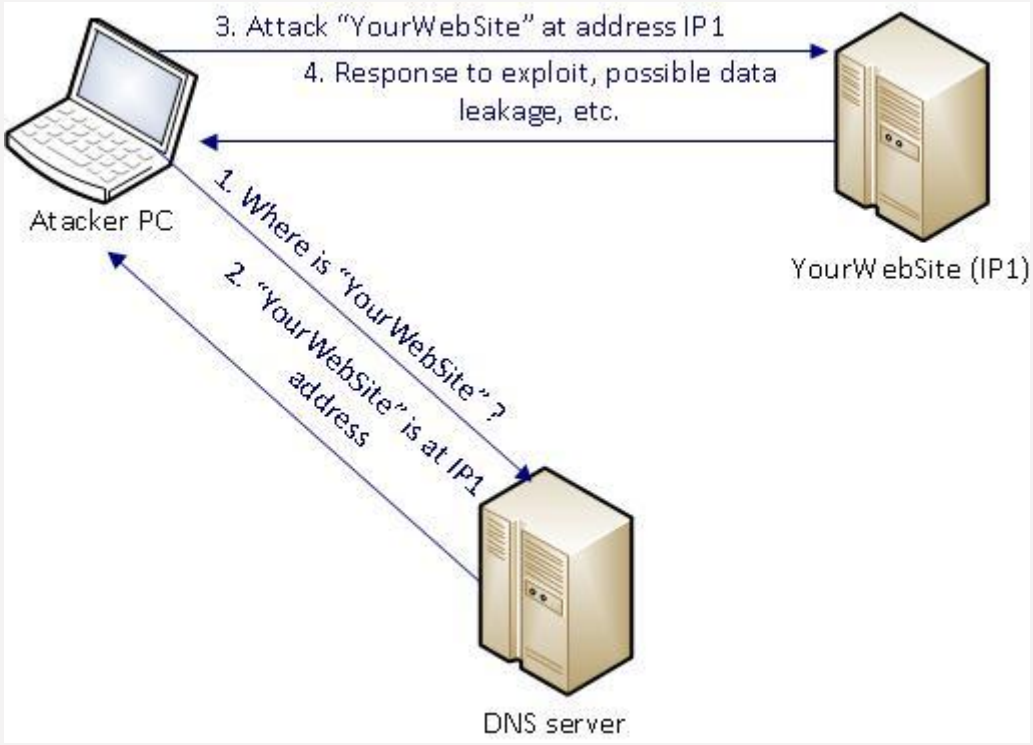
Intrusions in most cases are stealthy and happens when no one expects them

DEFENSE of WEBSITES

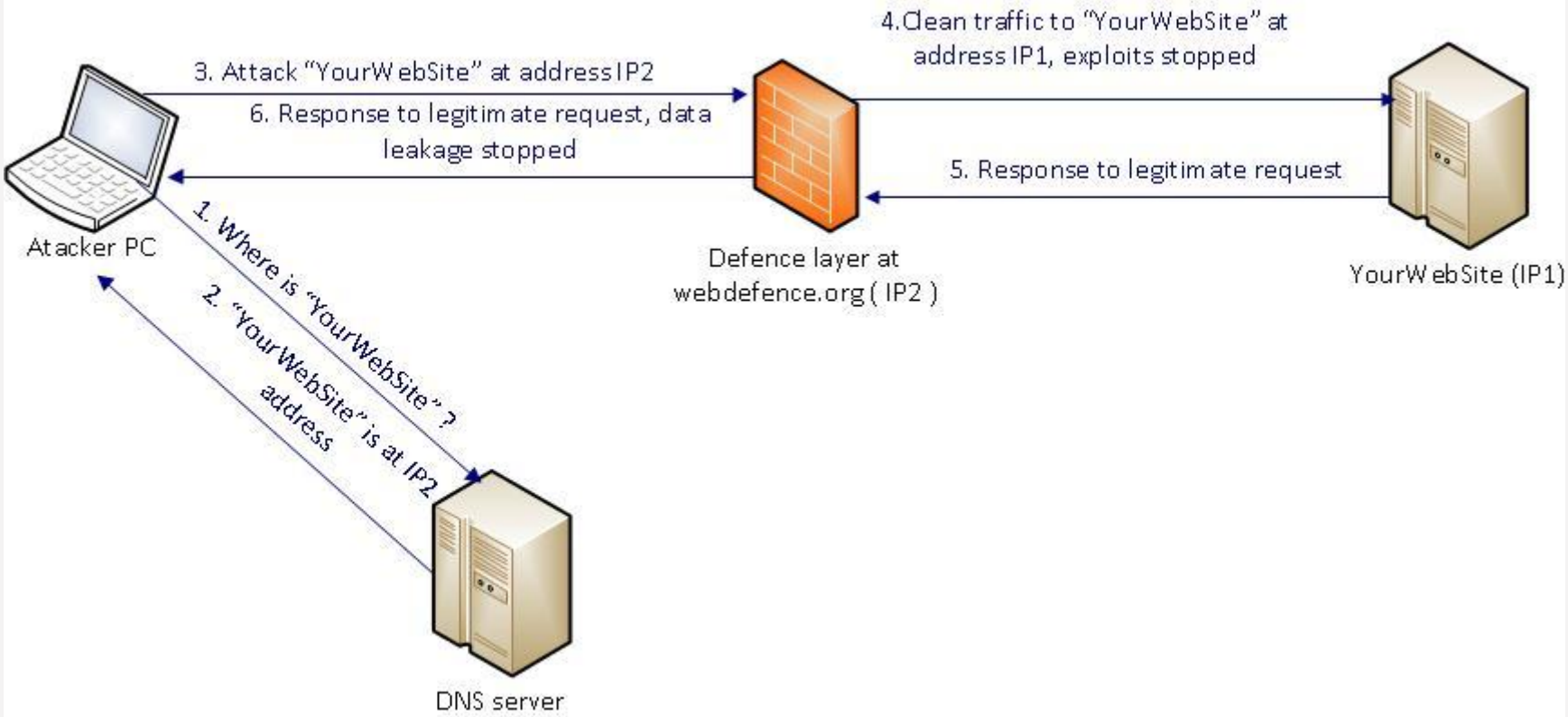
While defending website there are 2 mandatory steps in order to succeed:

- Pentests
- Web application firewalls

BEFORE WEB APPLICATION FIREWALL



AFTER WEB APPLICATION FIREWALL



HOW TO DEFEND A WEBSITE ?

Let's have a look at the main techniques for defending website using web application firewall:

- Blacklist
- Whitelist
- Blacklist + Whitelist
- Entry control
- Parameter control

HOW TO DEFEND A WEBSITE ?

- “Spying” user
- XSS defense
- Bruteforce defense
- Scoring defense profile violations
- Error cloacking
- Reaction

BLACKLIST

Blacklist defense is a signature based defense. This is the simplest and fastest approach to defend against most popular attacks. New attacks or attacks for which there are no signatures will not be detected. E.g. illegal connection to website administration panel will not be detected.

BLACKLIST

This is the most common approach to defend websites. It is also the cheapest one, but not the most secure.

https://www.vrk.lt/?testas=1%27%20or%201=1%20--

Edit   REMOTE_ADDR @eq 188.69.192.154

23 events, page: 1

	Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message	
☐	Wm4vpTImQP	28.01.2018 22:16:37	lb_ngwaf modsecurity	28.01.2018 22:16:37	??		CRITICAL Score: -1	IP: 188.69.192.154 Country: LT Port: 33442	Method: GET Host: www.[redacted]lt URI: / Response: 302	SQL Injection Attack Detected via libinjection	Rule: 942100
☐	Wm4vpTImQP	28.01.2018 22:16:37	lb_ngwaf modsecurity	28.01.2018 22:16:37	??		CRITICAL Score: -1	IP: 188.69.192.154 Country: LT Port: 33442	Method: GET Host: www.[redacted]lt URI: / Response: 302	SQL Injection Attack Detected via libinjection	Rule: 942100
☐	Wm4vpTImQP	28.01.2018 22:16:37	lb_ngwaf modsecurity	28.01.2018 22:16:37	??		CRITICAL Score: -1	IP: 188.69.192.154 Country: LT Port: 33442	Method: GET Host: www.[redacted]lt URI: / Response: 302	SQL Injection Attack Detected via libinjection	Rule: 942100

WHITELIST

- Let’s assume that web application firewall allows only some requests which are predefined in advance. All other requests are simply dropped. In this case web application firewall works in so called “whitelist mode”
- “Whitelist mode” – it requires much more effort to configure but the result is better then using “blacklist mode”

1 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
WoqyaQr4QA	19.02.2018 13:18:01	www_vrk_lt_waf1 modsecurity	19.02.2018 13:18:02	??		Score: -1	IP: 94.130.108.59 Country: UA Port: 28624	Method: GET Host: www.vrk.lt URI: /invoice/report/1 Response: 302	Request URL not in profile Rule: 10

WHITELIST + BLACKLIST

It is possible to defend website using mixed WHITELIST + BLACKLIST approach – in this case the defense is better then compared to a single blacklist or whitelist approach.

ENTRY CONTROL

- This defense technique blocks all requests untill a visitor is unauthenticated
- This is a very effective approach to stop anonymous / unauthenticated attacks

ENTRY CONTROL

https://org.rinkejopuslapis.lt/test

525 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
WoqZuVw@jH	19.02.2018 11:32:41	org_vrk modsecurity	19.02.2018 11:32:41	??		Score: -1	IP: 54.37.85.61 Country: US Port: 52771	Method: GET Host: org.rinkejopuslapis.lt URI: /documents/10434/49903/DTS+naudotojo+vadovas.docx/646f5dce-cdc6-4fef-97a6-0bdb6fcdc8f4 Response: 302	Entry control violation - user not logged in Rule: 405
WoqZsVw@jH	19.02.2018 11:32:33	org_vrk modsecurity	19.02.2018 11:32:34	??		Score: -1	IP: 54.37.85.61 Country: US Port: 52717	Method: GET Host: org.rinkejopuslapis.lt URI: /robots.txt Response: 302	Entry control violation - user not logged in Rule: 405
WoqXflw@jH	19.02.2018 11:23:10	org_vrk modsecurity	19.02.2018 11:23:11	??		Score: -1	IP: 216.244.66.235 Country: US Port: 48793	Method: GET Host: org.rinkejopuslapis.lt URI: /robots.txt Response: 302	Entry control violation - user not logged in Rule: 405
WoqTQlw@jH	19.02.2018 11:05:06	org_vrk modsecurity	19.02.2018 11:05:07	??		Score: -1	IP: 84.46.168.9 Country: LT Port: 41478	Method: GET Host: org.rinkejopuslapis.lt URI: /rp-theme/images/favicon.ico Response: 302	Entry control violation - user not logged in Rule: 405
WoqNXVw@jH	19.02.2018 10:39:57	org_vrk modsecurity	19.02.2018 10:39:58	??		Score: -1	IP: 78.56.235.71 Country: LT Port: 30822	Method: GET Host: org.rinkejopuslapis.lt URI: /rp-theme/images/favicon.ico Response: 302	Entry control violation - user not logged in Rule: 405
							IP: 78.56.235.71	Method: GET Host: org.rinkejopuslapis.lt	Entry control

PARAMETER CONTROL

- http://www.vrk.lt/home?arg1=1

PARAMETER CONTROL (name)

PARAMETER CONTROL (value)

16 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
WokquQr4QA	18.02.2018 09:26:49	www_vrk_lt_waf1 modsecurity	18.02.2018 09:26:50	??		Score: -1	IP: 207.46.13.164 Country: US Port: 17236	Method: GET Host: www.vrk.lt URI: /en/2016-seimo/rezultatai Response: 302	Unallowed argument srcurl value Rule: 20
WokquQr4QA	18.02.2018 09:26:49	www_vrk_lt_waf1 modsecurity	18.02.2018 09:26:50	??		Score: -1	IP: 207.46.13.164 Country: US Port: 17236	Method: GET Host: www.vrk.lt URI: /en/2016-seimo/rezultatai Response: 302	Unallowed argument srcurl value Rule: 20
WoeAbwr4QA	17.02.2018 03:07:59	www_vrk_lt_waf1 modsecurity	17.02.2018 03:08:00	??		Score: -1	IP: 198.144.157.39 Country: US Port: 34088	Method: GET Host: www.vrk.lt URI: /pk686/dalyviai Response: 302	Unallowed argument srcurl value Rule: 20
Wob6FAr4QA	16.02.2018 17:34:44	www_vrk_lt_waf2 modsecurity	16.02.2018 17:34:45	??		Score: -1	IP: 54.36.148.13 Country: US Port: 53125	Method: GET Host: www.vrk.lt URI: /en/2016-seimo/rezultatai Response: 302	Unallowed argument srcurl value Rule: 20
Wob6FAr4QA	16.02.2018 17:34:44	www_vrk_lt_waf2 modsecurity	16.02.2018 17:34:45	??		Score: -1	IP: 54.36.148.13 Country: US Port: 53125	Method: GET Host: www.vrk.lt URI: /en/2016-seimo/rezultatai Response: 302	Unallowed argument srcurl value Rule: 20
WoZJwwr4QA	16.02.2018 05:02:27	www_vrk_lt_waf2 modsecurity	16.02.2018 05:02:28	??		Score: -1	IP: 104.254.245.106 Country: -- Port: 51970	Method: GET Host: www.vrk.lt URI: /en/taikytini-ikainiai-2017-mer	Unallowed argument srcurl value Rule: 20

PARAMETER CONTROL (value)

```
--WoNZ1wr4QAUAAHoiYOAAAAAN-A--
[13/Feb/2018:23:34:15 +0200] WoNZ1wr4QAUAAHoiYOAAAAAN 35.227.103.175 35765 10.248.64.5 80
--WoNZ1wr4QAUAAHoiYOAAAAAN-B--
GET /taikytini-ikainiai-2017-mer?
p_p_id=82&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&_82_struts_action=%2Flanguage%2Fview'A=0&_82_redirect=%2Ftaikyt
ikainiai-2017-mer%3FsrcUrl%3DreklamIkainiai%2FkampIkainiaiHtml%253FpkId%253D964%2526zpId%253D5409&languageId=en_GB
HTTP/1.1
Accept-Encoding: gzip
CF-IPCountry: US
CF-RAY: 3ecae92391a09fc6-IAD
X-Forwarded-Proto: http
CF-Visitor: {"scheme":"http"}
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pt-PT; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2 (.NET CLR
3.5.30729)
Referer: http://www.vrk.lt/taikytini-ikainiai-2017-mer?
p_p_id=82&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&_82_struts_action=%2Flanguage%2Fview'A=0&_82_redirect=%2Ftaikyt
ikainiai-2017-mer%3FsrcUrl%3DreklamIkainiai%2FkampIkainiaiHtml%253FpkId%253D964%2526zpId%253D5409&languageId=en_GB
Content-Type: text/html; charset=utf-8
CF-Connecting-IP: 35.227.103.175
X-Mentainance: False
X-Forwarded-For: 35.227.103.175
x-allow-ip: false
```

“SPYING” USER

It is possible to interpret in a human understandable way the requests that the website visitor performs. In this case you can see visitor actions at a high level

“SPYING” USER

45 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
Wop6P1w@jH	19.02.2018 09:18:23	org_vrk modsecurity	19.02.2018 09:18:24	??		Score: -1	IP: 88.119.96.174 Country: LT Port: 65463	Method: POST Host: org.rinkejopuslapis.lt URI: /prisijungti Response: 302	Evaldzia Client authentication successfull Rule: 404
Wop4T1w@jH	19.02.2018 09:10:07	org_vrk modsecurity	19.02.2018 09:10:08	??		Score: -1	IP: 88.119.96.174 Country: LT Port: 62277	Method: POST Host: org.rinkejopuslapis.lt URI: /prisijungti Response: 302	Client disconnected Rule: 402
WopxlVw@jH	19.02.2018 08:41:26	org_vrk modsecurity	19.02.2018 08:41:26	??		Score: -1	IP: 88.119.96.174 Country: LT Port: 52844	Method: POST Host: org.rinkejopuslapis.lt URI: /prisijungti Response: 302	Evaldzia Client authentication successfull Rule: 404
WoVOl1w@jH	15.02.2018 11:10:47	org_vrk modsecurity	15.02.2018 11:10:48	??		Score: -1	IP: 88.119.96.174 Country: LT Port: 61741	Method: POST Host: org.rinkejopuslapis.lt URI: /prisijungti Response: 302	Evaldzia Client authentication successfull Rule: 404
WoVLBlw@jH	15.02.2018 10:55:34	org_vrk modsecurity	15.02.2018 10:55:35	??		Score: -1	IP: 88.119.96.174 Country: LT Port: 56635	Method: POST Host: org.rinkejopuslapis.lt URI: /prisijungti Response: 302	Evaldzia Client authentication successfull Rule: 404
WoVKZFw@jH	15.02.2018 10:52:52	org_vrk modsecurity	15.02.2018 10:52:52	??		Score: -1	IP: 88.119.96.174 Country: LT Port: 55322	Method: POST Host: org.rinkejopuslapis.lt URI: /prisijungti Response: 302	Evaldzia Client authentication successfull Rule: 404
WoRYfFw@jH	14.02.2018 17:40:44	org_vrk modsecurity	14.02.2018 17:40:45	??		Score: -1	IP: 88.119.96.174 Country: LT Port: 52003	Method: POST Host: org.rinkejopuslapis.lt URI: /prisijungti Response: 302	Client disconnected Rule: 402
							IP: 88.119.96.174	Method: POST Host: org.rinkejopuslapis.lt	

XSS DEFENSE

- XSS attack – one of the most dangerous attacks against users for websites which contains financial or personal data
- It’s possible to tune web application firewall in a way that XSS attacks becomes impossible

Edit SENSOR_ID @eq 27 RULE_ID @eq !910000 RULE_ID @eq 604

32 events, page: 8

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
WmmcamwtF3	25.01.2018 10:59:22	eshop_ngwaf modsecurity	25.01.2018 10:59:22	??		Score: -1	IP: 193.219.87.239 Country: LT Port: 33640	Method: GET Host: [redacted].lt URI: /shop/view/2-pm-viln-np Response: 302	Possible session hijacking: Expected session address 84.15.180.50 but got 193.219.87.239 Rule: 604
WmmR2q5f-e	25.01.2018 10:14:18	eshop_ngwaf modsecurity	25.01.2018 10:14:18	??		Score: -1	IP: 66.102.8.218 Country: US Port: 48307	Method: GET Host: [redacted].lt URI: /assets/4845a9db/css/fonts/RobotoSlab/stylesheet.css Response: 302	Possible session hijacking: Expected session address 66.102.8.214 but got 66.102.8.218 Rule: 604

BRUTE FORCE DEFENSE

Edit REMOTE_ADDR @eq 10.0.26.17

3 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
Wm7dQ0kVI7	29.01.2018 10:37:23	eshop_nzwaf modsecurity	29.01.2018 10:37:23	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted].lt URI: /login/in Response: 302	Enforcing earlier IP address block for 1 hour Rule: 5
Wm7dQUkVI7	29.01.2018 10:37:21	eshop_nzwaf modsecurity	29.01.2018 10:37:21	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted].lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dQUkVI7	29.01.2018 10:37:21	eshop_nzwaf modsecurity	29.01.2018 10:37:21	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: GET Host: [redacted] URI: /site/captcha Response: 200	Brute force detection - blocking for 15 min Rule: 412
Wm7dPkkVI7	29.01.2018 10:37:18	eshop_nzwaf modsecurity	29.01.2018 10:37:18	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted].lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dO0kVI7	29.01.2018 10:37:15	eshop_nzwaf modsecurity	29.01.2018 10:37:15	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted].lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dGCOQAj	29.01.2018 10:36:40	eshop_nzwaf modsecurity	29.01.2018 10:36:40	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48136	Method: POST Host: [redacted].lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dCnmAIX	29.01.2018 10:36:26	eshop_nzwaf modsecurity	29.01.2018 10:36:26	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48132	Method: POST Host: [redacted].lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7c72j4eR	29.01.2018 10:35:59	eshop_nzwaf modsecurity	29.01.2018 10:35:59	??		Score: -1	IP: 10.0.26.17 Country: --	Method: POST Host: [redacted].lt URI: /login/in	Login failure Rule: 405

SCORING DEFENSE PROFILE

Edit REMOTE_ADDR @eq 10.0.26.17

3 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
Wm7dQ0kVI7	29.01.2018 10:37:23	eshop_nzwaf modsecurity	29.01.2018 10:37:23	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted] lt URI: /login/in Response: 302	Enforcing earlier IP address block for 1 hour Rule: 5
Wm7dQUkVI7	29.01.2018 10:37:21	eshop_nzwaf modsecurity	29.01.2018 10:37:21	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted] lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dQUkVI7	29.01.2018 10:37:21	eshop_nzwaf modsecurity	29.01.2018 10:37:21	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: GET Host: [redacted] URI: /site/captcha Response: 200	Brute force detection - blocking for 15 min Rule: 412
Wm7dPkkVI7	29.01.2018 10:37:18	eshop_nzwaf modsecurity	29.01.2018 10:37:18	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted] lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dO0kVI7	29.01.2018 10:37:15	eshop_nzwaf modsecurity	29.01.2018 10:37:15	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48200	Method: POST Host: [redacted] lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dGCOQAj	29.01.2018 10:36:40	eshop_nzwaf modsecurity	29.01.2018 10:36:40	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48136	Method: POST Host: [redacted] lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7dCnmAIX	29.01.2018 10:36:26	eshop_nzwaf modsecurity	29.01.2018 10:36:26	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48132	Method: POST Host: [redacted] lt URI: /login/in Response: 200	Login failure Rule: 405
Wm7c72j4eR	29.01.2018 10:35:59	eshop_nzwaf modsecurity	29.01.2018 10:35:59	??		Score: -1	IP: 10.0.26.17 Country: -- Port: 48106	Method: POST Host: [redacted] lt URI: /login/in Response: 200	Login failure Rule: 405

ERROR CLOACKING

- Errors that websites discloses to the visitors should be hidden. If the visitor encounters an error it is possible to redirect visitor to the main website page

https://www.vrk.lt/css/print.css

404 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
Woq7PAr4QA	19.02.2018 13:55:40	www_vrk_lt_waf2 modsecurity	19.02.2018 13:55:41	??		Score: -1	IP: 94.130.108.59 Country: UA Port: 62665	Method: GET Host: www.vrk.lt URI: /css/print.css Response: 302	Cloacking Rule: 1
Woq3RAr4QA	19.02.2018 13:38:44	www_vrk_lt_waf1 modsecurity	19.02.2018 13:38:45	??		Score: -1	IP: 195.182.69.130 Country: LT Port: 37575	Method: GET Host: www.vrk.lt URI: /css/print.css Response: 302	Cloacking Rule: 1
Woq0zAr4QA	19.02.2018 13:28:12	www_vrk_lt_waf2 modsecurity	19.02.2018 13:28:13	??		Score: -1	IP: 204.79.180.5 Country: US Port: 49247	Method: GET Host: www.vrk.lt URI: /css/print.css Response: 302	Cloacking Rule: 1
Woqp4Qr4QA	19.02.2018 12:41:37	www_vrk_lt_waf1 modsecurity	19.02.2018 12:41:38	??		Score: -1	IP: 158.129.132.180 Country: LT Port: 11581	Method: GET Host: www.vrk.lt URI: /css/print.css Response: 302	Cloacking Rule: 1
WoqeMQr4QA	19.02.2018 11:51:45	www_vrk_lt_waf1 modsecurity	19.02.2018 11:51:45	??		Score: -1	IP: 163.172.66.19 Country: GB Port: 52120	Method: GET Host: www.vrk.lt URI: /css/print.css Response: 302	Cloacking Rule: 1
WoqaNgr4QA	19.02.2018 11:34:46	www_vrk_lt_waf2 modsecurity	19.02.2018 11:34:46	??		Score: -1	IP: 165.225.84.90 Country: US Port: 61491	Method: GET Host: www.vrk.lt URI: /css/print.css	Cloacking Rule: 1

REACTION

- At the moment that an ongoing attack has been identified it should be stopped immediately. It can be a block for offending IP address for some time.

https://www.vrk.lt/phpmyadmin.php

364 events, page: 1

Event ID	Date	Sensor	Received	Site	Tags	Severity	Source	Destination	Message
Woq7yQr4QA	19.02.2018 13:58:01	www_vrk_lt_waf2 modsecurity	19.02.2018 13:58:01	??		Score: -1	IP: 94.130.108.59 Country: UA Port: 63479	Method: GET Host: www.vrk.lt URI: /phpmyadmin.php Response: 302	You should not access any PHP file - block it for 1 hour Rule: 8
WoqtCQr4QA	19.02.2018 12:55:05	www_vrk_lt_waf1 modsecurity	19.02.2018 12:55:06	??		Score: -1	IP: 113.128.104.212 Country: CN Port: 17424	Method: GET Host: www.vrk.lt URI: /ogShow.aspx Response: 302	You should not access any PHP file - block it for 1 hour Rule: 8
WoqbUQr4QA	19.02.2018 11:39:29	www_vrk_lt_waf2 modsecurity	19.02.2018 11:39:29	??		Score: -1	IP: 124.225.46.114 Country: CN Port: 63913	Method: GET Host: www.vrk.lt URI: /ogShow.aspx Response: 302	You should not access any PHP file - block it for 1 hour Rule: 8
WoqFJAr4QA	19.02.2018 10:04:52	www_vrk_lt_waf1 modsecurity	19.02.2018 10:04:53	??		Score: -1	IP: 220.175.60.228 Country: CN Port: 65300	Method: GET Host: www.vrk.lt URI: /ogPipe.aspx Response: 302	You should not access any PHP file - block it for 1 hour Rule: 8
WoqFEQr4QA	19.02.2018 10:04:33	www_vrk_lt_waf2 modsecurity	19.02.2018 10:04:34	??		Score: -1	IP: 175.152.28.178 Country: CN Port: 18446	Method: GET Host: www.vrk.lt URI: /ogPipe.aspx Response: 302	You should not access any PHP file - block it for 1 hour Rule: 8
WoqFCAr4QA	19.02.2018 10:04:24	www_vrk_lt_waf1 modsecurity	19.02.2018 10:04:25	??		Score: -1	IP: 124.235.138.236 Country: CN Port: 65086	Method: GET Host: www.vrk.lt URI: /ogShow.aspx Response: 302	You should not access any PHP file - block it for 1 hour Rule: 8

RESULTS

- While using all above mentioned defense techniques it becomes extremely difficult for an attacker to takeover a website

- All shown defense techniques can be implemented using “open source” software.

RESULTS

- All shown defense techniques does not require any website modifications – i.e. the defense is transparent.

SOME DEMOS

Questions?