RIPE

Reducing “Unwanted/Bad” traffic

Jeroen Leendertz, 19-05-2022

Biggest benefits

No more captcha
Less overall power consumption

Room for improvement

But in my opinion best of all

Less opportunities for hackers

SUBMISSIONS

Vinder | My Elementor

Alle (564) | Unread (466) | Read (98)

Search...

Bulk actions | Apply | All Pages | All Forms | All Time

564 items « ‹ 1 of 12 › » Export All to CSV

Main	Actions Status	Form	Page	ID	Submission Date
[redacted]	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	581	mei 18, 2022 1:51 pm
[redacted]	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	580	mei 17, 2022 6:36 pm
[redacted]	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	579	mei 17, 2022 4:30 pm
[redacted]	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	578	mei 17, 2022 11:46 am
cryptotrustfull@yandex.com	✓	**New Form (49d5695)**	**Contact | Hoveniersbedrijf Smolders**	**577**	**mei 17, 2022 4:13 am**
eric.jones.z.mail@gmail.com	✓	**New Form (49d5695)**	**Contact | Hoveniersbedrijf Smolders**	**576**	**mei 17, 2022 1:15 am**
eric.jones.z.mail@gmail.com	✓	**New Form (49d5695)**	**Contact | Hoveniersbedrijf Smolders**	**575**	**mei 16, 2022 11:30 pm**
elinedirven@live.nl	✓	**New Form (49d5695)**	**Contact | Hoveniersbedrijf Smolders**	**574**	**mei 16, 2022 7:49 pm**
koenenjennysouren@gmail.com	✓	**New Form (49d5695)**	**Contact | Hoveniersbedrijf Smolders**	**573**	**mei 16, 2022 4:24 pm**

	eric.jones.z.mail@gmail.com	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	556	mei 15, 2022 12:02 am
	eesddwardlroms@gmail.com	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	555	mei 14, 2022 12:49 pm
	[redacted]	✓	New Form (8efb7f2)	Hoveniersbedrijf Smolders | voor al u...	554	mei 14, 2022 12:34 pm
	xrkingkpb@yandex.ru	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	553	mei 14, 2022 8:54 am
	contabo_mer@outlook.com	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	552	mei 14, 2022 2:02 am
	l29bj@course-fitness.com	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	551	mei 13, 2022 9:50 pm
	eric.jones.z.mail@gmail.com	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	550	mei 13, 2022 9:20 pm
	3eoa80r0@hotmail.com	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	549	mei 13, 2022 2:25 pm
	[redacted]	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	548	mei 13, 2022 8:23 am
	[redacted] View | Trash | Mark as Unread	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	547	mei 11, 2022 11:04 am
	[redacted]	✓	New Form (49d5695)	Contact | Hoveniersbedrijf Smolders	546	mei 10, 2022 8:34 am

localhost:8388

+ New ▶ Run Chart → Follow Save Input Data {} Insert jeroe

Welcome! * houthandeltilburg.nl.sx

```
1  LIST(['file:/C:/Users/jeroe/Documents/*houthandeltilburg.nl.log'])
2  | parse(pattern:"
3  (IPADDR:clientIp | [! \n]+):host
4  ' ' ('-' | NSPACE:ident)                          // Apache auth is vulnerable to the
5  ' ' ('-' | (DATA{1,8096}:auth >>(' [' HTTPDATE))) // log poisoning attach via auth field
6  ' ' '[' HTTPDATE:timestamp ']'
7  ' ' (('\"' [A-Z-_]+:verb ' ' LD{0,8096}:uri ' HTTP/' FLOAT:httpversion '\"') | DQS:invalidRequest)
8  ' ' INTEGER:response
9  ' ' (LONG:bytes | '-')
10 (' ' DQS:referrer (' ' DQS:agent)?)?
11        EOL")
12        | select(*  unmatched)
```

SUCCEEDED parser(451786665 bytes, 273790 unmatched, 0,06%) RESULT: 1.434.678 rows (483MB) disk write: 483MB duration: 1.756

Results Explanation Query log (2)

0 - 99999 1

#	clientIp	host	ident	auth	timestamp	verb	uri	httpversio	inva
0	37.187.72.216	37.187.72.216	NULL	NULL	2022-03-22 00:42:38.000 +0100	GET	/.well-known/acme-challenge/143288bfa5b5dc2463109f6e2ad5b52ekey	1.0	NULL
1	37.187.72.216	37.187.72.216	NULL	NULL	2022-03-22 00:42:57.000 +0100	GET	/.well-known/acme-challenge/b61293419c851b4adcaba82cfcd75bbckey	1.0	NULL
2	18.159.196.172	18.159.196.172	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
3	18.116.86.117	18.116.86.117	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
4	66.133.109.36	66.133.109.36	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
5	52.39.4.59	52.39.4.59	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
6	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:12.000 +0100	POST	/wp-admin/admin-ajax.php	1.1	NULL
7	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:18.000 +0100	POST	/wp-admin/admin-ajax.php	1.1	NULL
8	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:21.000 +0100	GET	/winkel/toebehoren-2/overige-producten/drukverdeelplaat-o-70mm/	1.1	NULL
9	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:26.000 +0100	GET	/wp-admin/tools.php?page=redirection.php&sub=options	1.1	NULL
10	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-content/plugins/redirection/redirection.js?ver=5.2.3-cb109e7c800603ff2d5cc098451320be	1.1	NULL
11	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-json/redirection/v1/setting/?_wpnonce=16ad77ba8d	1.1	NULL
12	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-content/uploads/2021/12/favicon-houthandel-100x100.png	1.1	NULL
13	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-content/uploads/2021/12/favicon-houthandel.png	1.1	NULL
14	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:33.000 +0100	POST	/wp-admin/admin-ajax.php	1.1	NULL

/system/patterns/houthandeltilburg.nl.sx

localhost:8388

+ New ▶ Run Chart → Follow Save Input Data {} Insert jeroe

Welcome! * houthandeltilburg.nl.sx

```
1  LIST(['file:/C:/Users/jeroe/Documents/*houthandeltilburg.nl.log'])
2  | parse(pattern:"
3  (IPADDR:clientIp | [! \n]+):host
4  ' ' ('-' | NSPACE:ident)                          // Apache auth is vulnerable to the
5  ' ' ('-' | (DATA{1,8096}:auth >>(' [' HTTPDATE))) // log poisoning attach via auth field
6  ' ' '[' HTTPDATE:timestamp ']'
7  ' ' (('\"' [A-Z-_]+:verb ' ' LD{0,8096}:uri ' HTTP/' FLOAT:httpversion '\"') | DQS:invalidRequest)
8  ' ' INTEGER:response
9  ' ' (LONG:bytes | '-')
10 (' ' DQS:referrer (' ' DQS:agent)?)?
11        EOL")
12        | select(*  unmatched)
```

SUCCEEDED parser(451786665 bytes, 273790 unmatched, 0,06%) RESULT: 1.434.678 rows (483MB) disk write: 483MB duration: 1.756

Results Explanation Query log (2)

0 - 99999 1

#	clientIp	host	ident	auth	timestamp	verb	uri	httpversio	inva
0	37.187.72.216	37.187.72.216	NULL	NULL	2022-03-22 00:42:38.000 +0100	GET	/.well-known/acme-challenge/143288bfa5b5dc2463109f6e2ad5b52ekey	1.0	NULL
1	37.187.72.216	37.187.72.216	NULL	NULL	2022-03-22 00:42:57.000 +0100	GET	/.well-known/acme-challenge/b61293419c851b4adcaba82cfcd75bbckey	1.0	NULL
2	18.159.196.172	18.159.196.172	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
3	18.116.86.117	18.116.86.117	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
4	66.133.109.36	66.133.109.36	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
5	52.39.4.59	52.39.4.59	NULL	NULL	2022-03-22 00:43:00.000 +0100	GET	/.well-known/acme-challenge/tNLc_vyTHB51rARCAOIC97RrslQ6lyJF3NO23v3ty8s	1.1	NULL
6	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:12.000 +0100	POST	/wp-admin/admin-ajax.php	1.1	NULL
7	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:18.000 +0100	POST	/wp-admin/admin-ajax.php	1.1	NULL
8	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:21.000 +0100	GET	/winkel/toebehoren-2/overige-producten/drukverdeelplaat-o-70mm/	1.1	NULL
9	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:26.000 +0100	GET	/wp-admin/tools.php?page=redirection.php&sub=options	1.1	NULL
10	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-content/plugins/redirection/redirection.js?ver=5.2.3-cb109e7c800603ff2d5cc098451320be	1.1	NULL
11	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-json/redirection/v1/setting/?_wpnonce=16ad77ba8d	1.1	NULL
12	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-content/uploads/2021/12/favicon-houthandel-100x100.png	1.1	NULL
13	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:27.000 +0100	GET	/wp-content/uploads/2021/12/favicon-houthandel.png	1.1	NULL
14	212.187.70.244	212.187.70.244	NULL	NULL	2022-03-22 00:43:22.000 +0100	POST	/wp-admin/admin-ajax.php	1.1	NULL

/system/patterns/houthandeltilburg.nl.sx

Questions?

RIPE