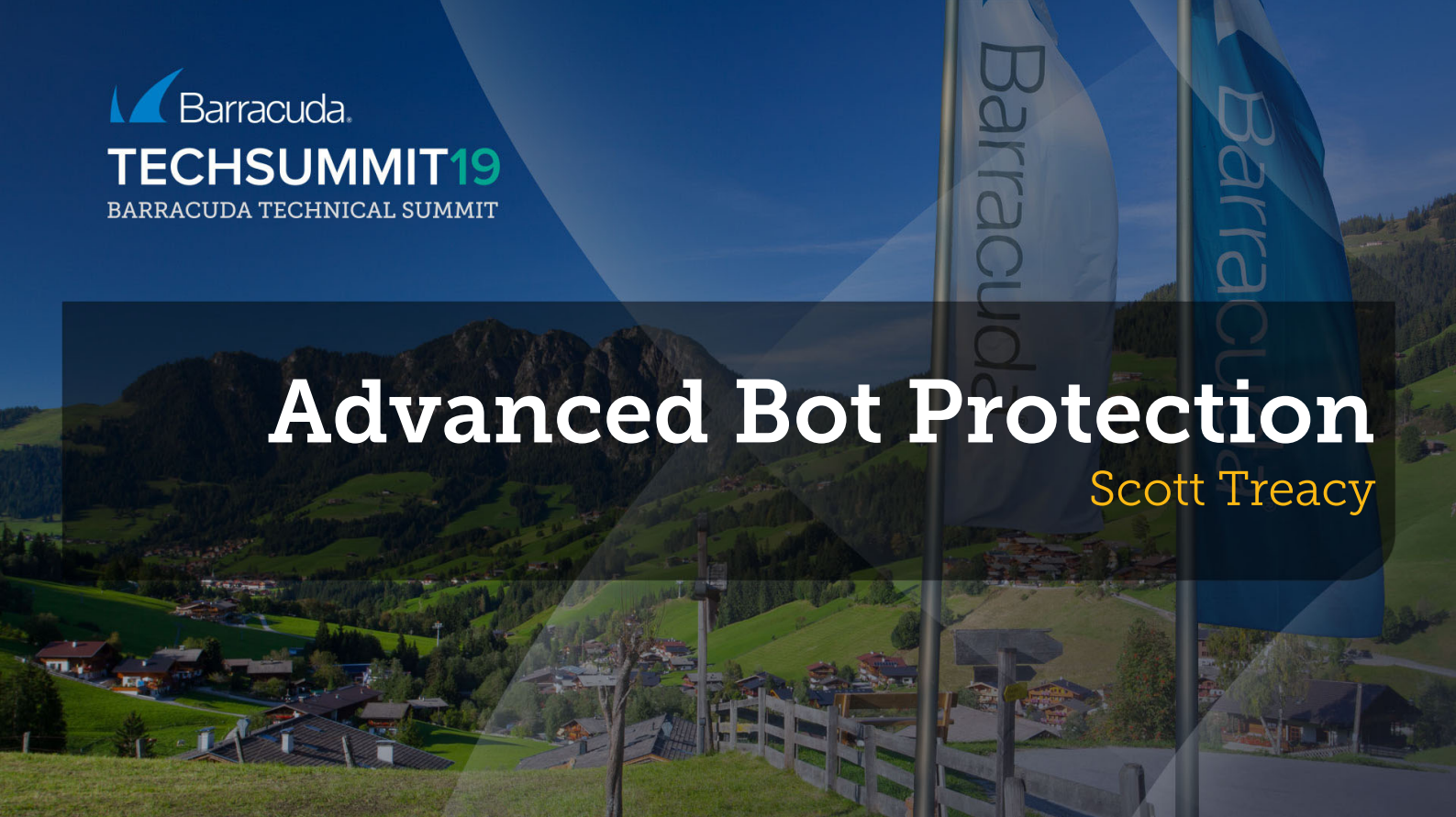

Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT
Advanced Bot Protection
Scott Treacy

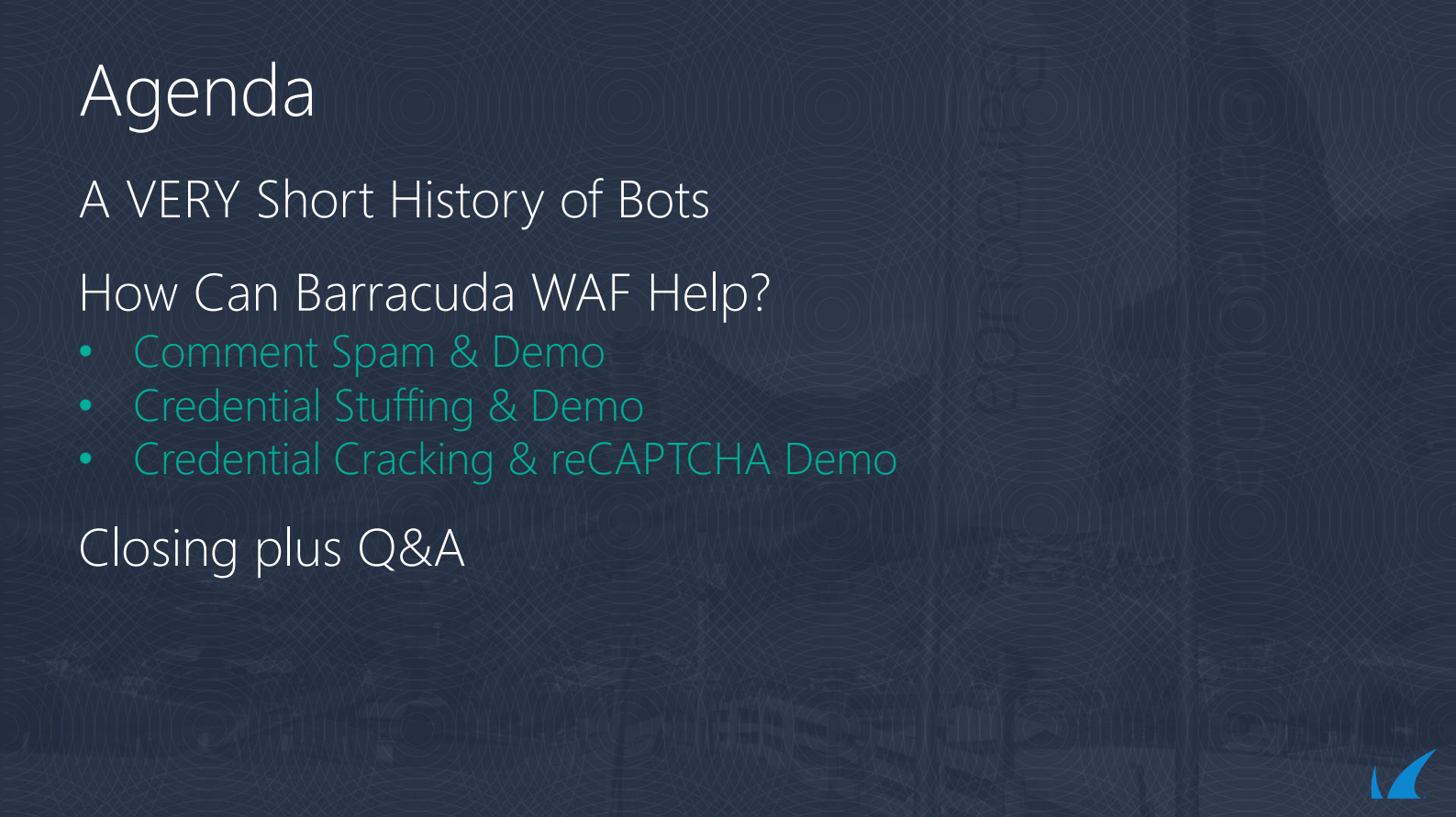
Agenda

A VERY Short History of Bots

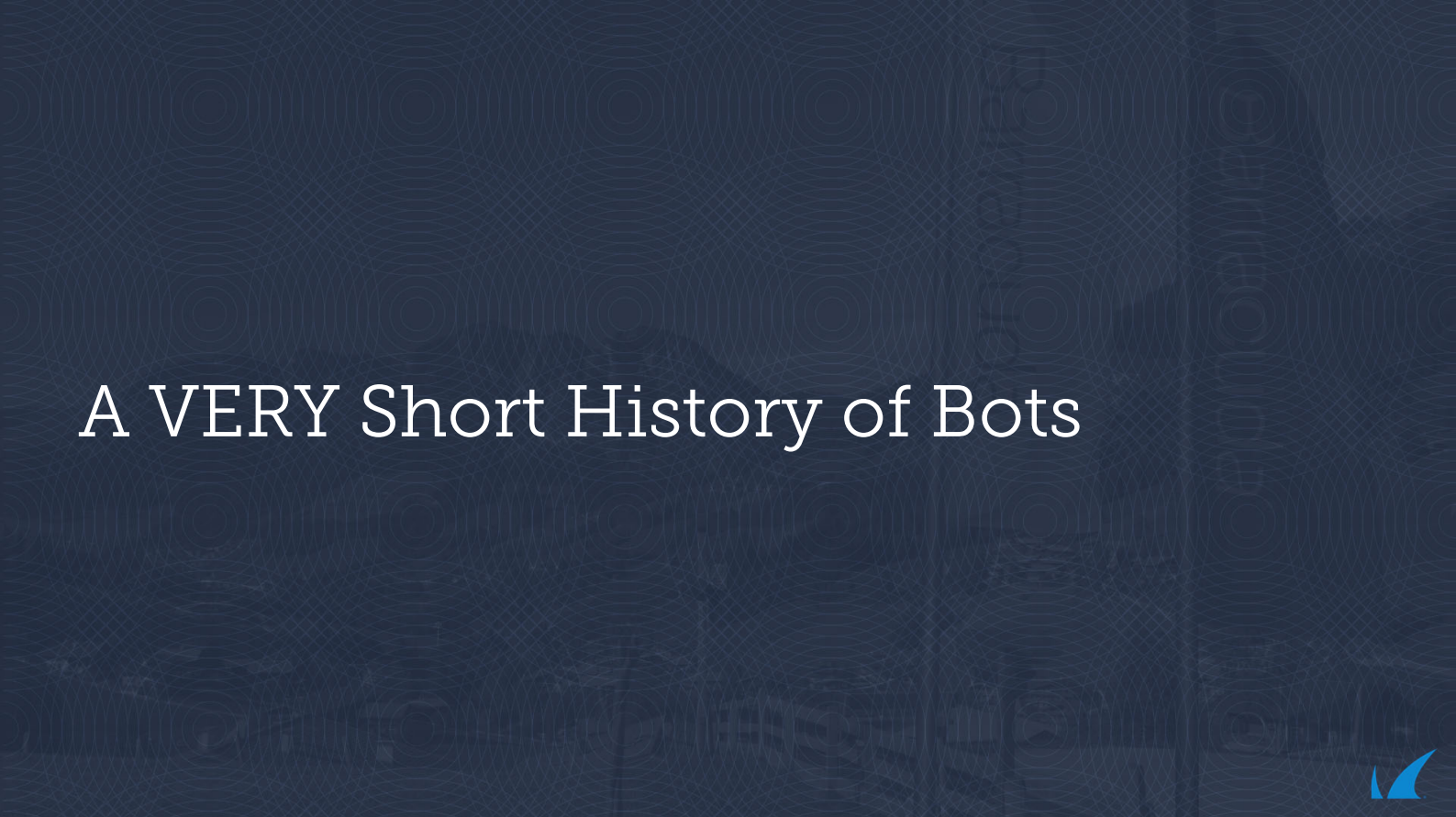
How Can Barracuda WAF Help?

- Comment Spam & Demo
- Credential Stuffing & Demo
- Credential Cracking & reCAPTCHA Demo

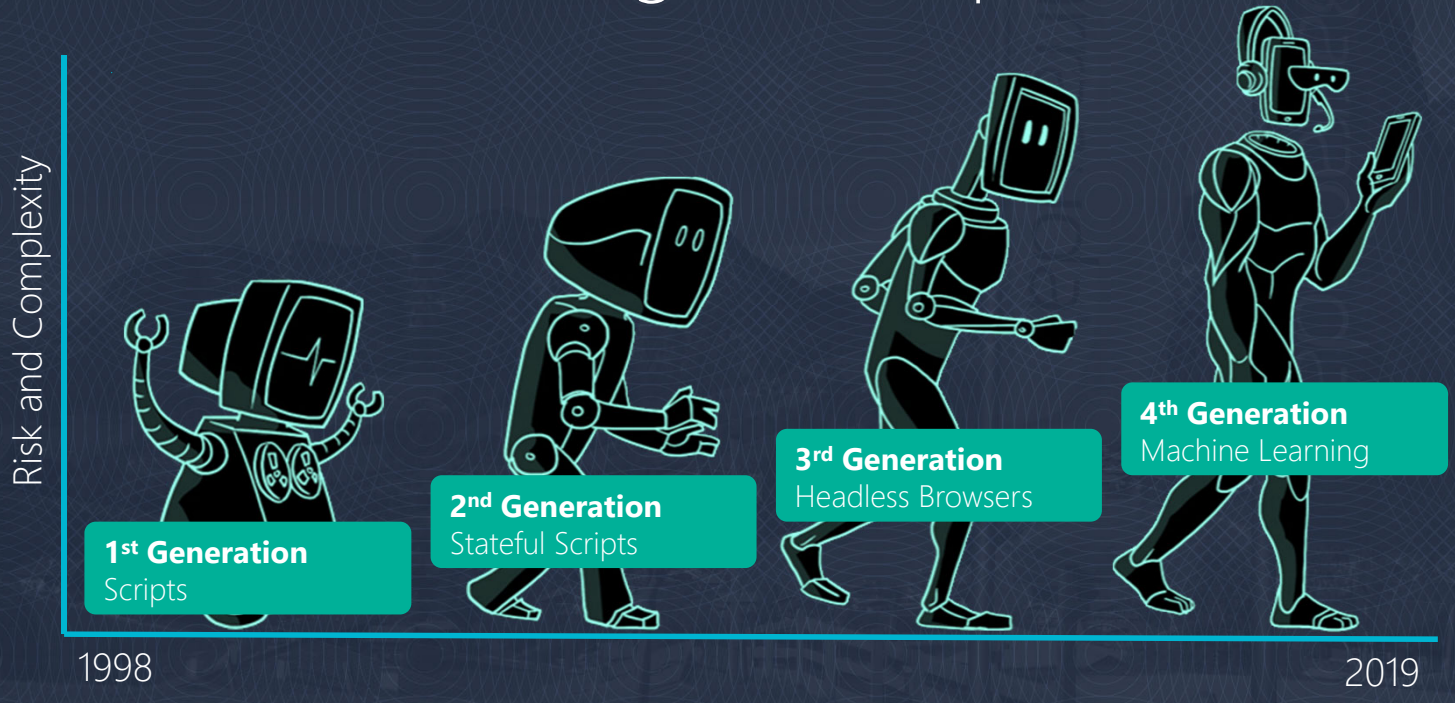
Closing plus Q&A



A VERY Short History of Bots



Bots are becoming more sophisticated



Vulnerabilities are being exploited !

Vulnerabilities are being exploited !

CBR
Computer Business Review

BA Facing £183.39M Fine for 2018 Data Breach

ED TARGETT EDITOR
8TH JULY 2019

WIRED

LILY HAY NEWMAN SECURITY 07.22.19 03:58 PM

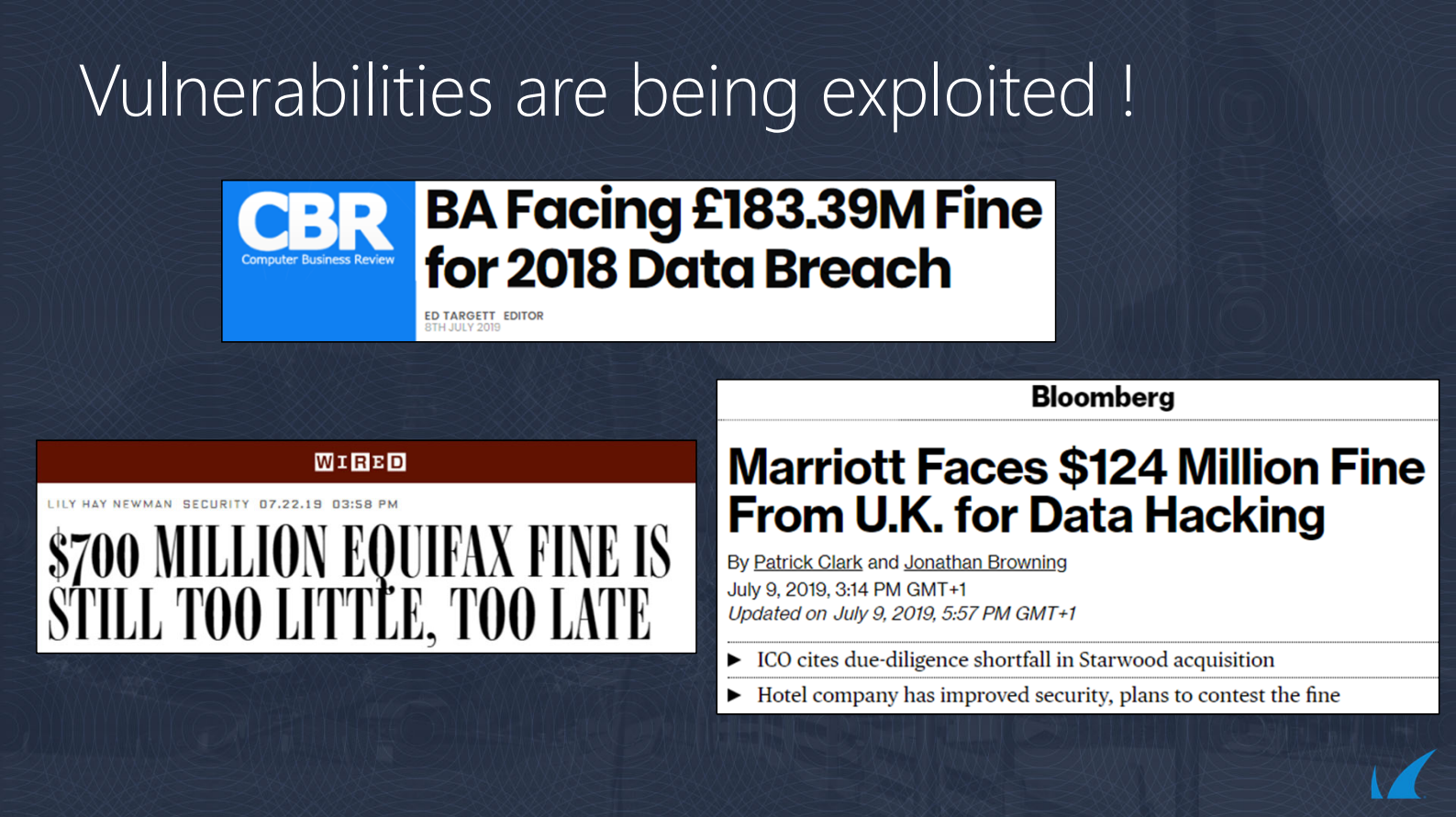
$700 MILLION EQUIFAX FINE IS STILL TOO LITTLE, TOO LATE

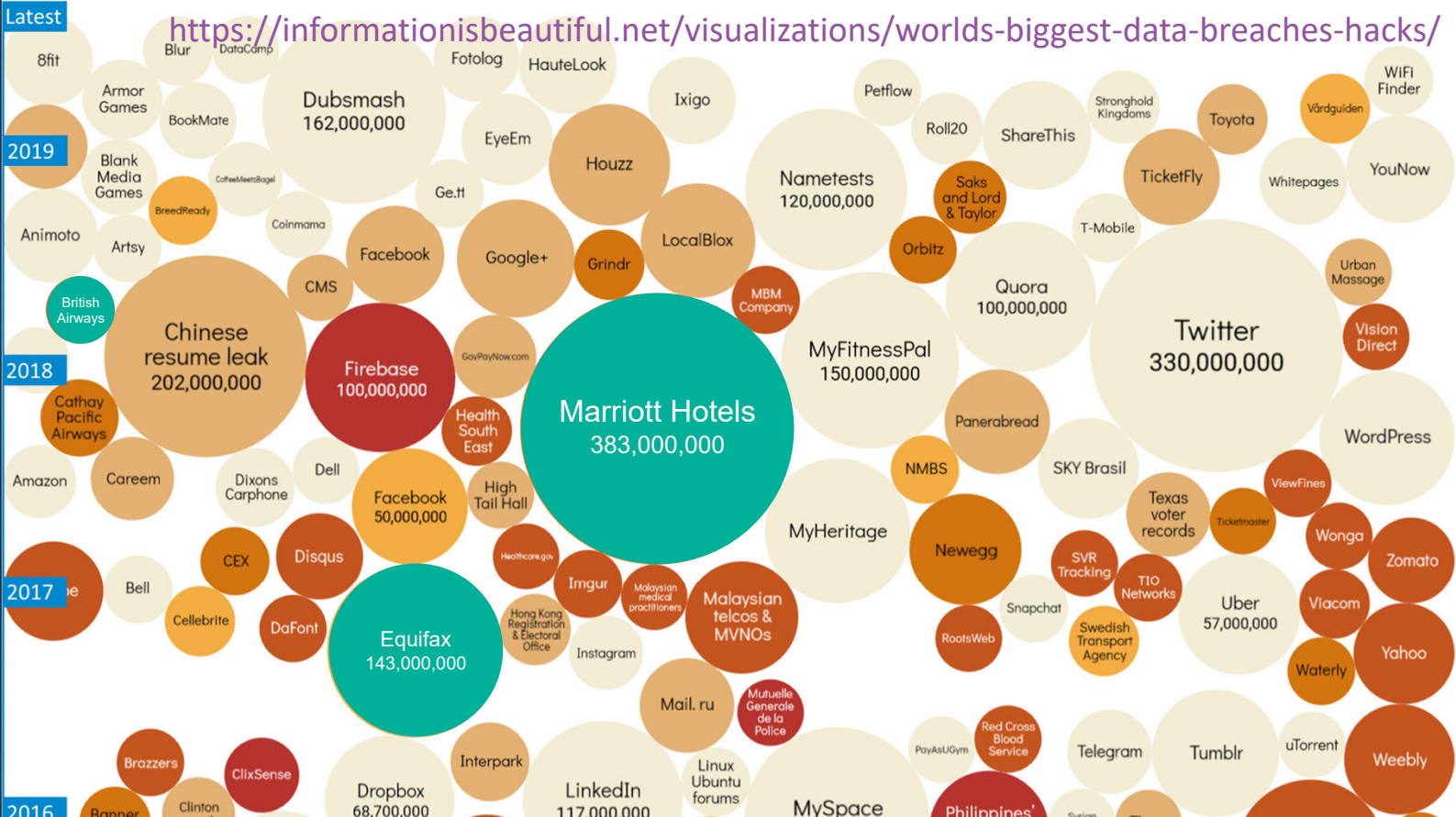
Bloomberg

Marriott Faces $124 Million Fine From U.K. for Data Hacking

By Patrick Clark and Jonathan Browning
July 9, 2019, 3:14 PM GMT+1
Updated on July 9, 2019, 5:57 PM GMT+1

- ICO cites due-diligence shortfall in Starwood acquisition
- Hotel company has improved security, plans to contest the fine




Latest
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
2019
2018
2017
2016
8fit
Blur
DataCamp
Fotolog
HauteLook
Armor Games
BookMate
Dubsmash
162,000,000
Ixigo
Petflow
Roll20
ShareThis
Stronghold Kingdoms
Toyota
WiFi Finder
Vårdguiden
EyeEm
Houzz
Nametests
120,000,000
Saks and Lord & Taylor
TicketFly
Whitepages
YouNow
Blank Media Games
CoffeeMeetsBagel
BreedReady
Ge.tt
Coinmama
Animoto
Artsy
Facebook
Google+
Grindr
LocalBlox
Orbitz
T-Mobile
Urban Massage
British Airways
CMS
Chinese resume leak
202,000,000
Firebase
100,000,000
GovPayNow.com
Marriott Hotels
383,000,000
MBM Company
MyFitnessPal
150,000,000
Quora
100,000,000
Twitter
330,000,000
Vision Direct
Cathay Pacific Airways
Health South East
Panerabread
WordPress
Amazon
Careem
Dixons Carphone
Dell
Facebook
50,000,000
High Tail Hall
NMBS
SKY Brasil
ViewFines
Texas voter records
Ticketmaster
Wonga
Zomato
CEX
Disqus
Healthcare.gov
Imgur
Malaysian medical practitioners
MyHeritage
Newegg
SVR Tracking
TIO Networks
Viacom
Bell
Cellebrite
DaFont
Equifax
143,000,000
Hong Kong Registration & Electoral Office
Instagram
Malaysian telcos & MVNOs
Snapchat
RootsWeb
Swedish Transport Agency
Uber
57,000,000
Waterly
Yahoo
Mail.ru
Mutuelle Generale de la Police
Brazzers
ClixSense
Interpark
Dropbox
68,700,000
LinkedIn
117,000,000
Linux Ubuntu forums
MySpace
PayAsUGym
Red Cross Blood Service
Telegram
Tumblr
uTorrent
Weebly
Clinton
Philippines'

How Can Barracuda WAF Help?

What did we have in v9…

Basic Bot Detection Tests

- Reverse DNS Lookups
- User-Agent Checks
- Honeytraps using various methods including robots.txt
- Device Detection (Computer versus Mobile)

Application DDoS Detection

- Various application layer DDoS detections
  - Brute Force attacks
  - Heavy URL attacks
  - Slow Client attacks etc.

WAF enhancements in v10…

Framework Enhancements

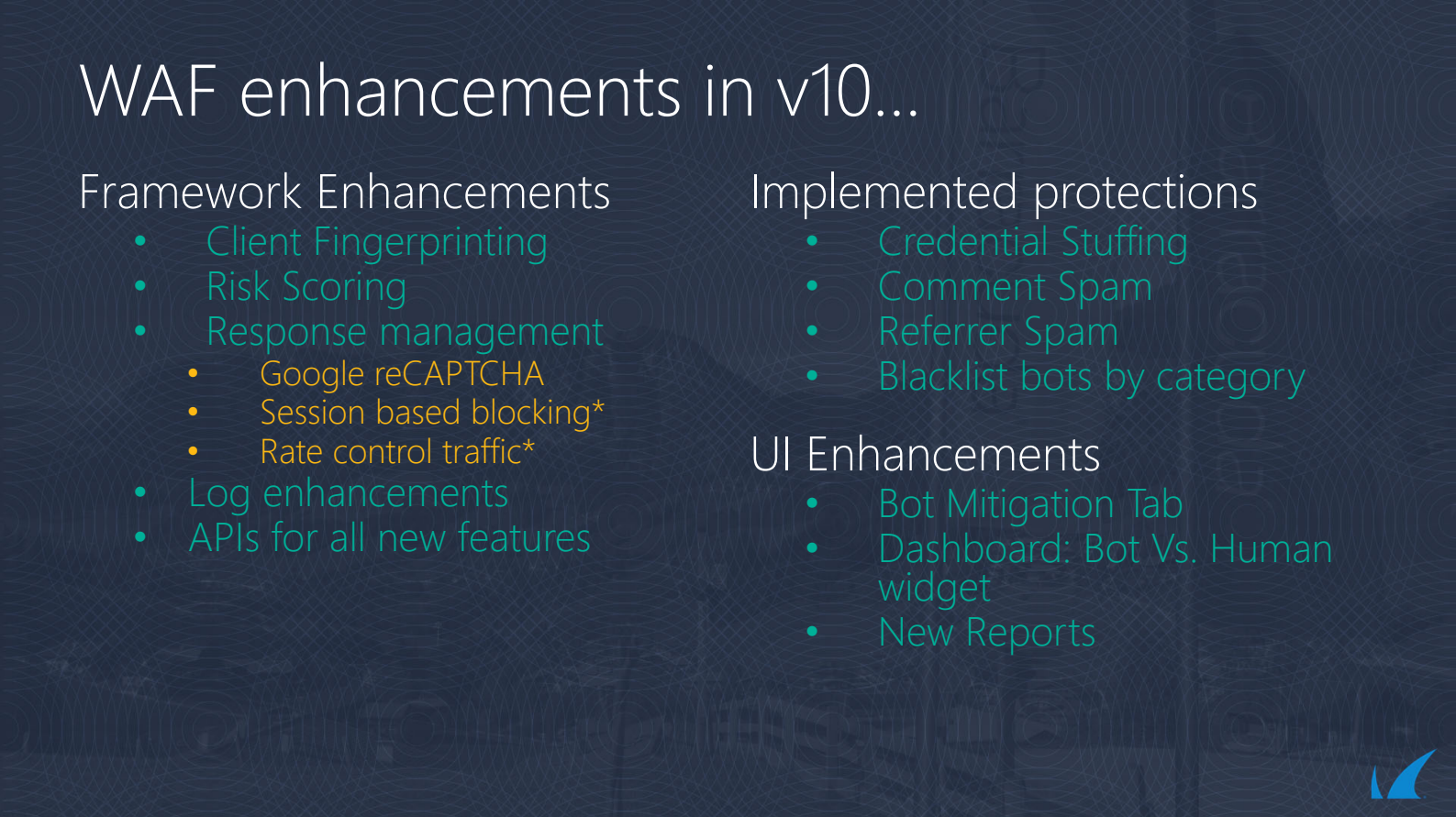
- Client Fingerprinting
- Risk Scoring
- Response management
  - Google reCAPTCHA
  - Session based blocking*
  - Rate control traffic*
- Log enhancements
- APIs for all new features

Implemented protections

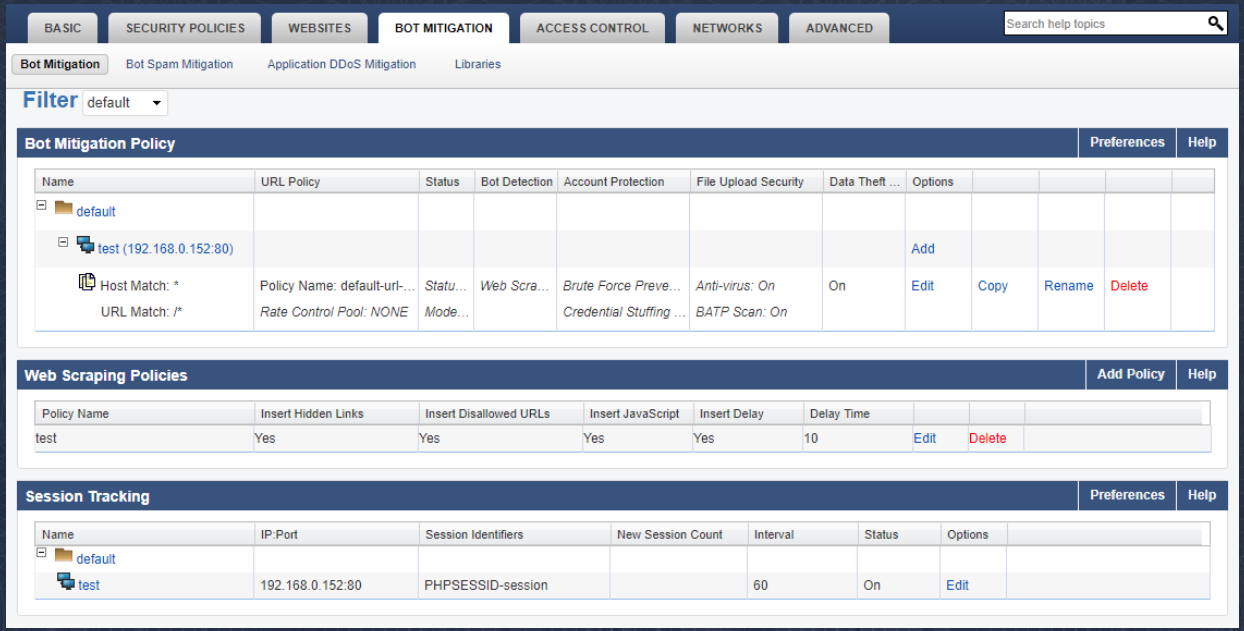
- Credential Stuffing
- Comment Spam
- Referrer Spam
- Blacklist bots by category

UI Enhancements

- Bot Mitigation Tab
- Dashboard: Bot Vs. Human widget
- New Reports

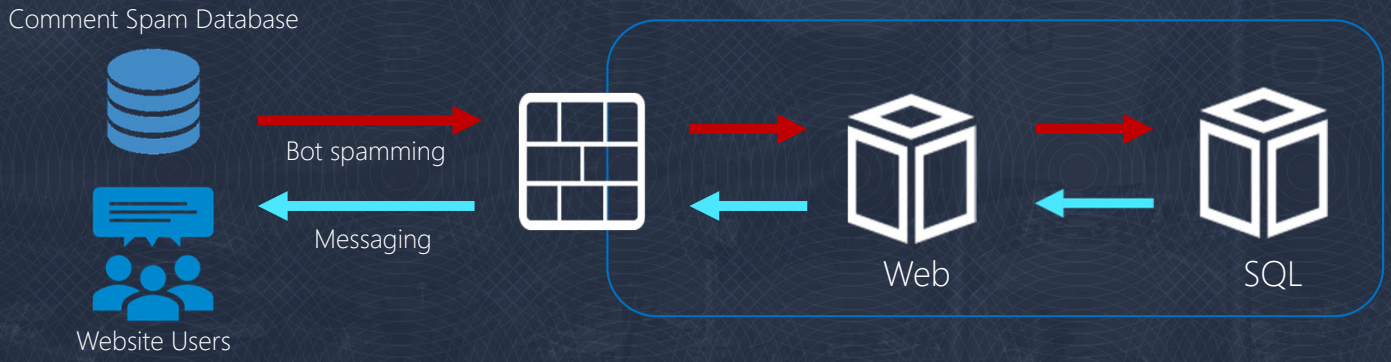


Bot Mitigation tab

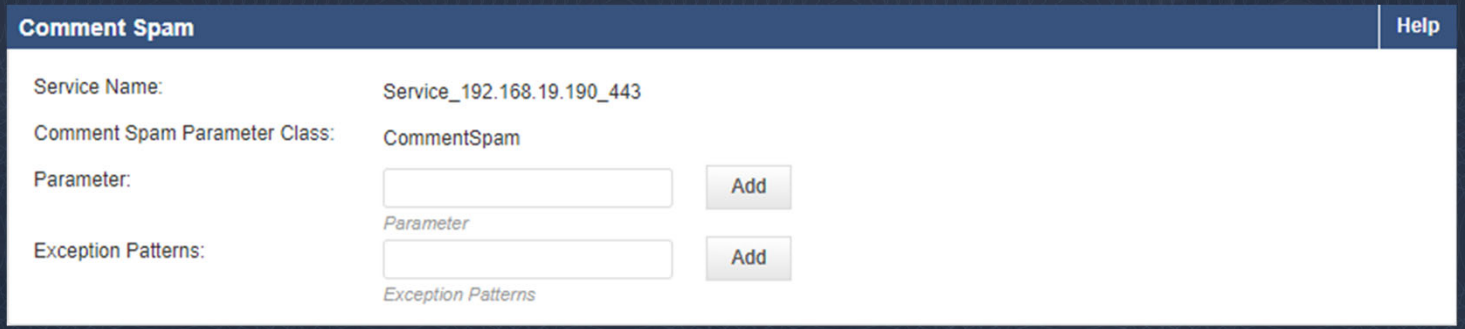


Comment Spamming

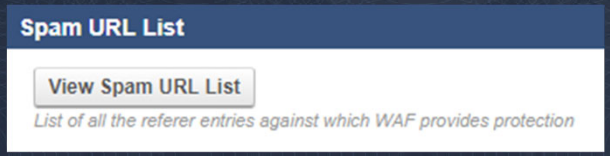
Lists of Comment Spam e.g. Politically motivated or advertising or malware are injected into discussion forums, guestbooks, comment and review sections of websites



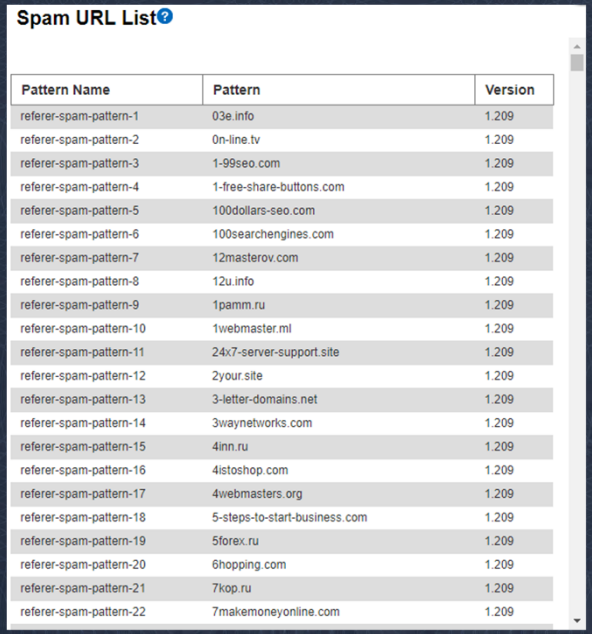
Comment Spam demo



The Comment Spam Database



View the Spam URL list



Spam URL List

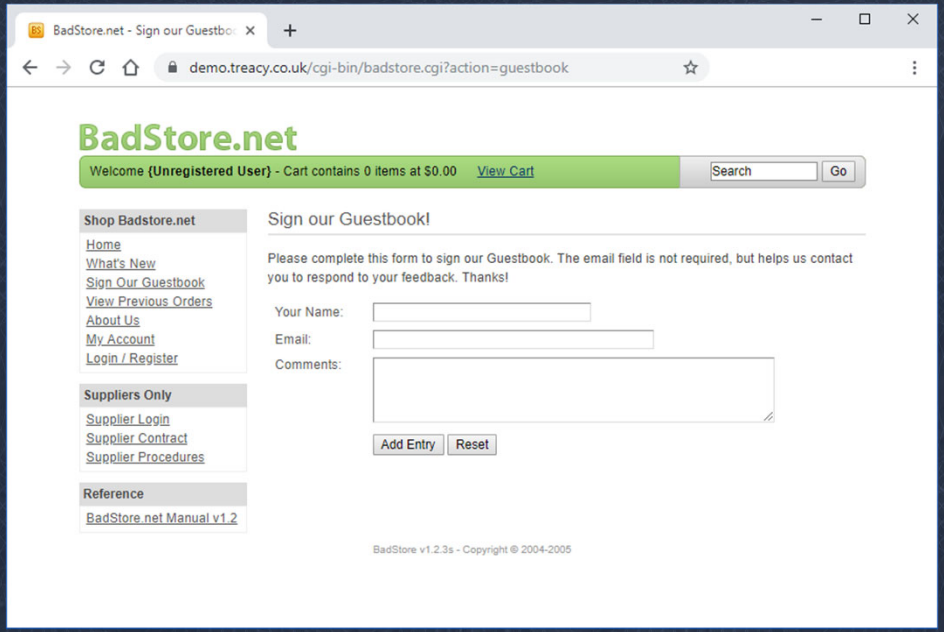
Pattern Name	Pattern	Version
referer-spam-pattern-1	03e.info	1.209
referer-spam-pattern-2	0n-line.tv	1.209
referer-spam-pattern-3	1-99seo.com	1.209
referer-spam-pattern-4	1-free-share-buttons.com	1.209
referer-spam-pattern-5	100dollars-seo.com	1.209
referer-spam-pattern-6	100searchengines.com	1.209
referer-spam-pattern-7	12masterov.com	1.209
referer-spam-pattern-8	12u.info	1.209
referer-spam-pattern-9	1pamm.ru	1.209
referer-spam-pattern-10	1webmaster.ml	1.209
referer-spam-pattern-11	24x7-server-support.site	1.209
referer-spam-pattern-12	2your.site	1.209
referer-spam-pattern-13	3-letter-domains.net	1.209
referer-spam-pattern-14	3waynetworks.com	1.209
referer-spam-pattern-15	4inn.ru	1.209
referer-spam-pattern-16	4istoshop.com	1.209
referer-spam-pattern-17	4webmasters.org	1.209
referer-spam-pattern-18	5-steps-to-start-business.com	1.209
referer-spam-pattern-19	5forex.ru	1.209
referer-spam-pattern-20	6hopping.com	1.209
referer-spam-pattern-21	7kop.ru	1.209
referer-spam-pattern-22	7makemoneyonline.com	1.209

Pick a Spam URL to test with

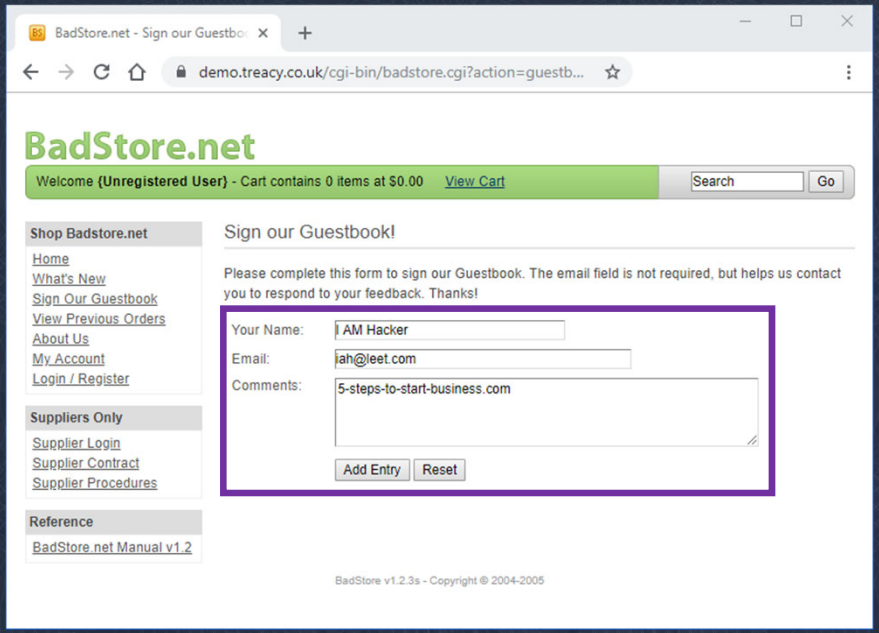
Spam URL List

Pattern Name	Pattern	Version
referer-spam-pattern-1	03e.info	1.209
referer-spam-pattern-2	0n-line.tv	1.209
referer-spam-pattern-3	1-99seo.com	1.209
referer-spam-pattern-4	1-free-share-buttons.com	1.209
referer-spam-pattern-5	100dollars-seo.com	1.209
referer-spam-pattern-6	100searchengines.com	1.209
referer-spam-pattern-7	12masterov.com	1.209
referer-spam-pattern-8	12u.info	1.209
referer-spam-pattern-9	1pamm.ru	1.209
referer-spam-pattern-10	1webmaster.ml	1.209
referer-spam-pattern-11	24x7-server-support.site	1.209
referer-spam-pattern-12	2your.site	1.209
referer-spam-pattern-13	3-letter-domains.net	1.209
referer-spam-pattern-14	3waynetworks.com	1.209
referer-spam-pattern-15	4inn.ru	1.209
referer-spam-pattern-16	4istoshop.com	1.209
referer-spam-pattern-17	4webmasters.org	1.209
referer-spam-pattern-18	5-steps-to-start-business.com	1.209
referer-spam-pattern-19	5forex.ru	1.209
referer-spam-pattern-20	6hopping.com	1.209
referer-spam-pattern-21	7kop.ru	1.209
referer-spam-pattern-22	7makemoneyonline.com	1.209

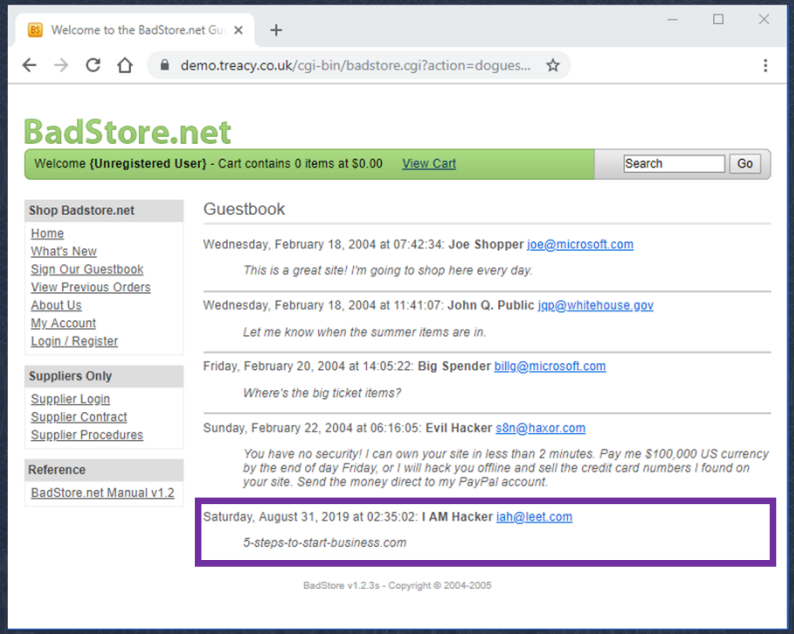
What pages do we need to protect?



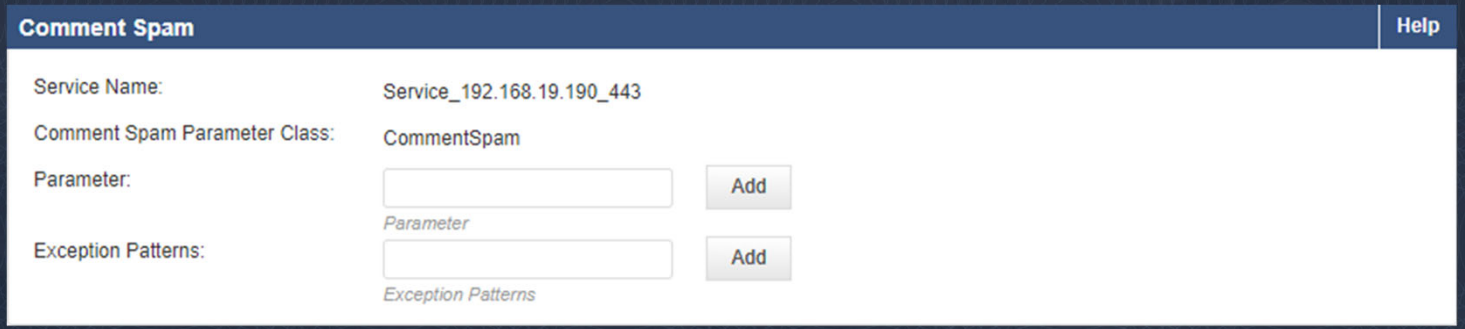
Testing using the comment spam URL



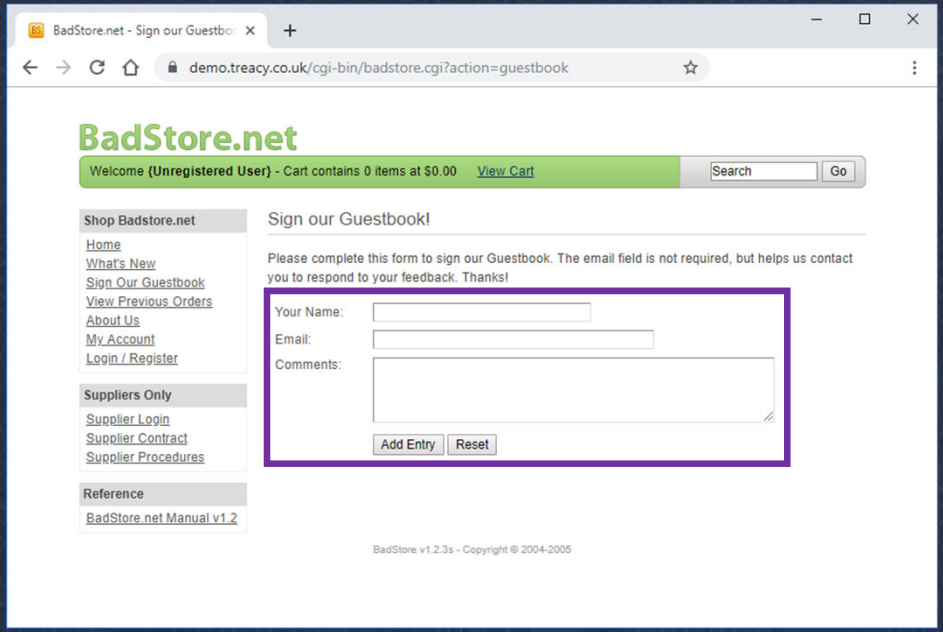
The BadStore Guestbook displays the Spam URL



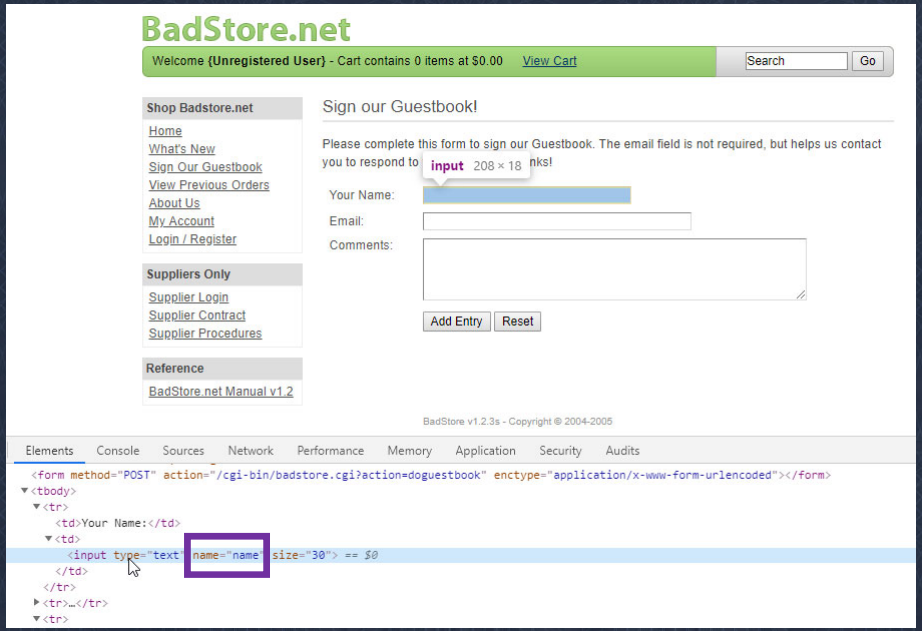
Comment Spam Parameters



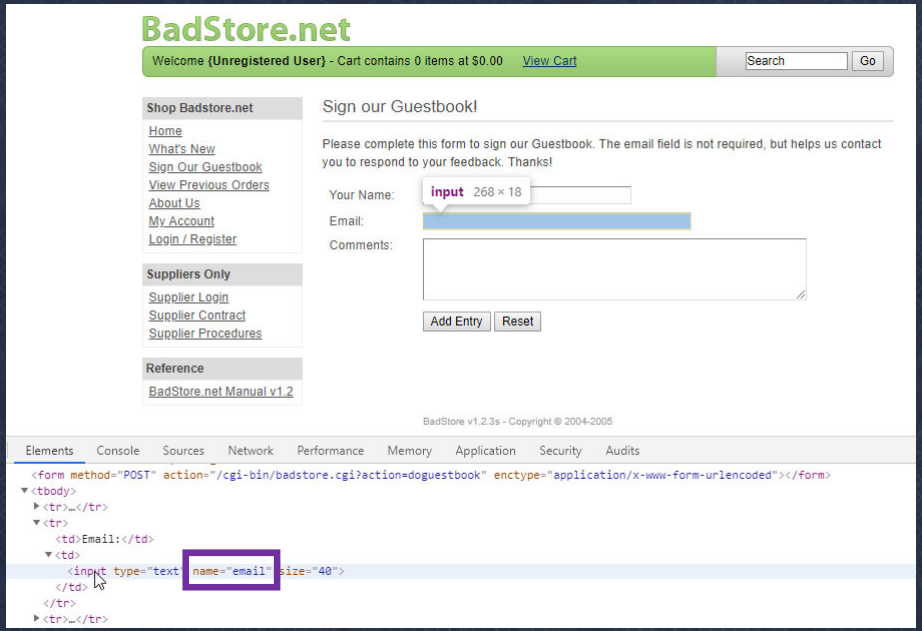
What are the comment field parameters?



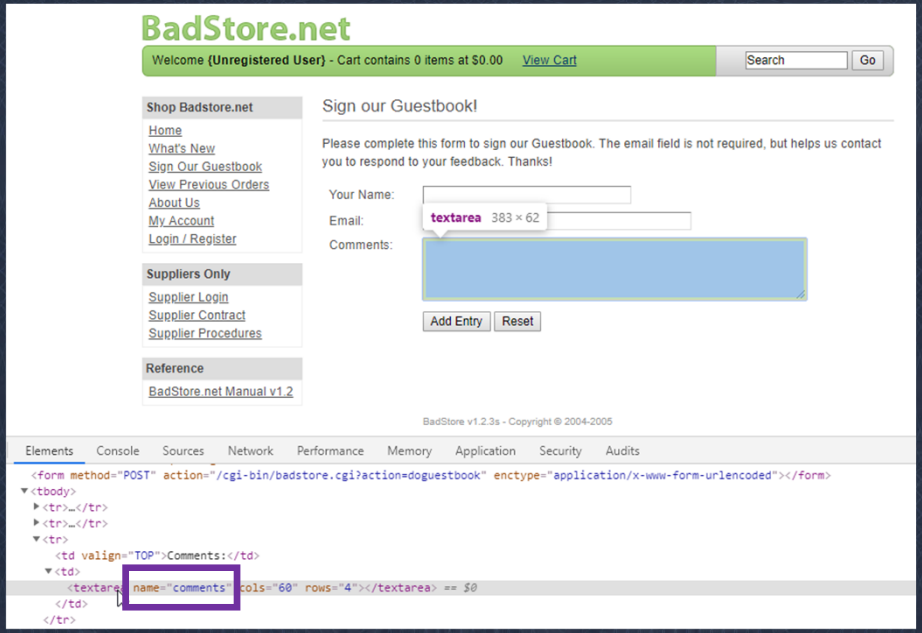
What is the Name parameter called?



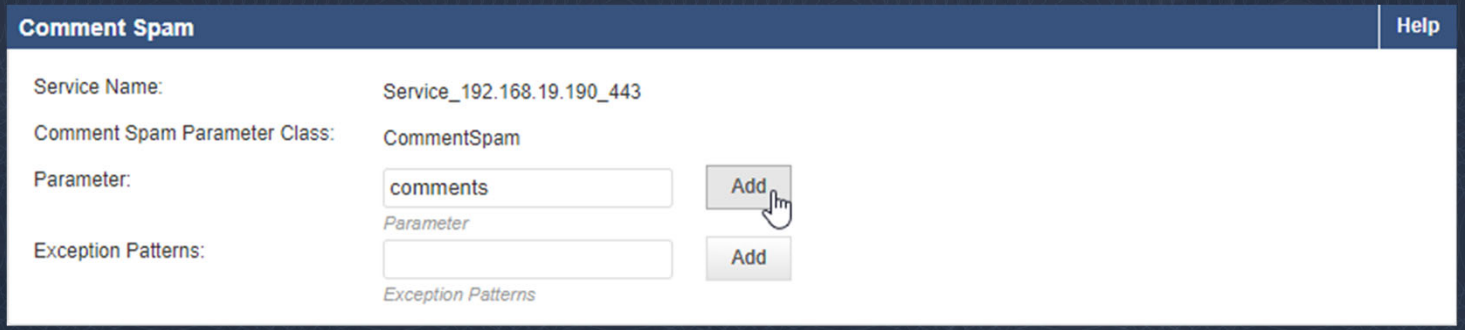
What is the Email parameter called?



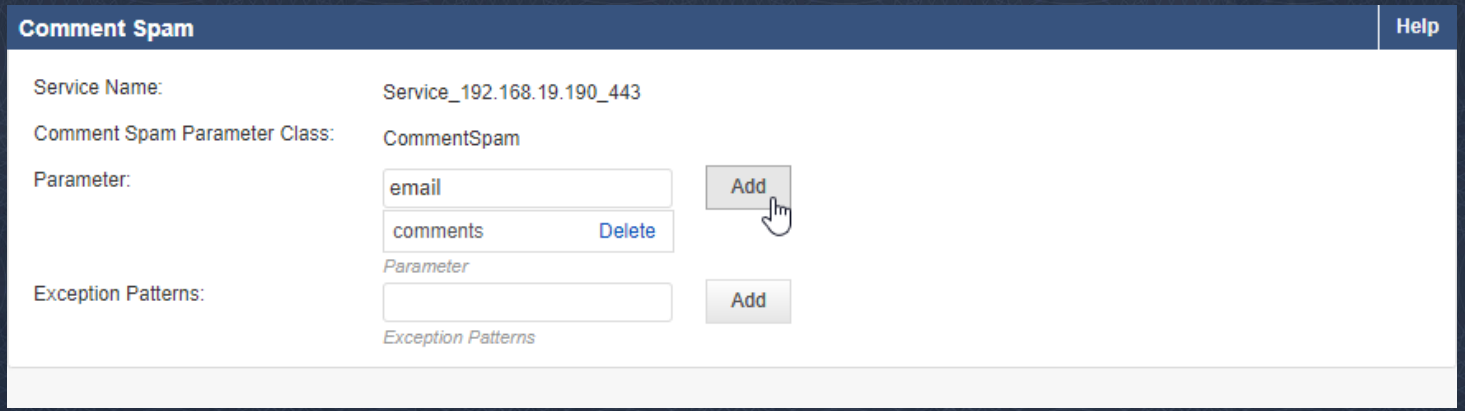
What is the Comments parameter called?



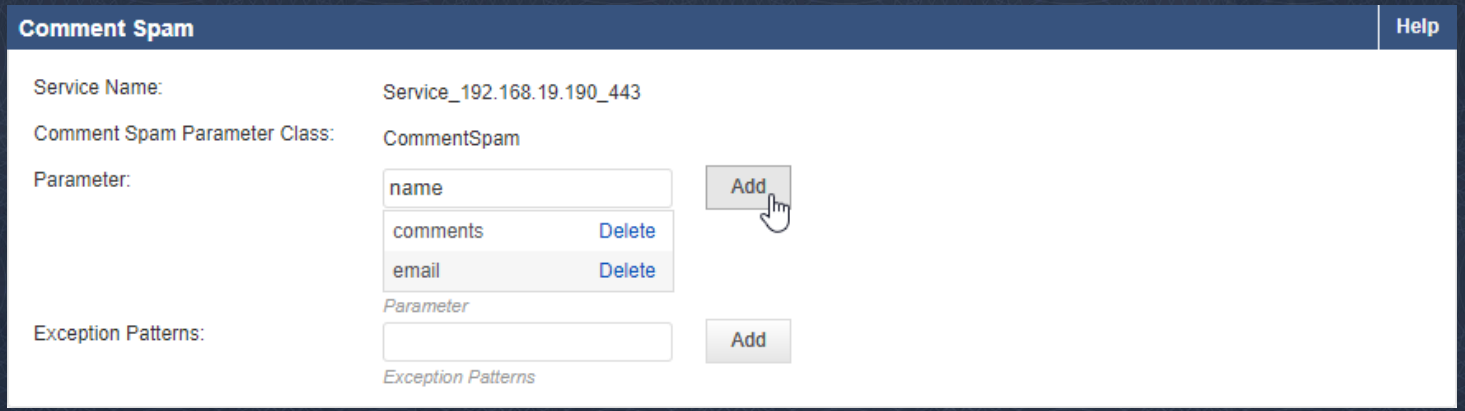
Comment Spam: Add the parameters



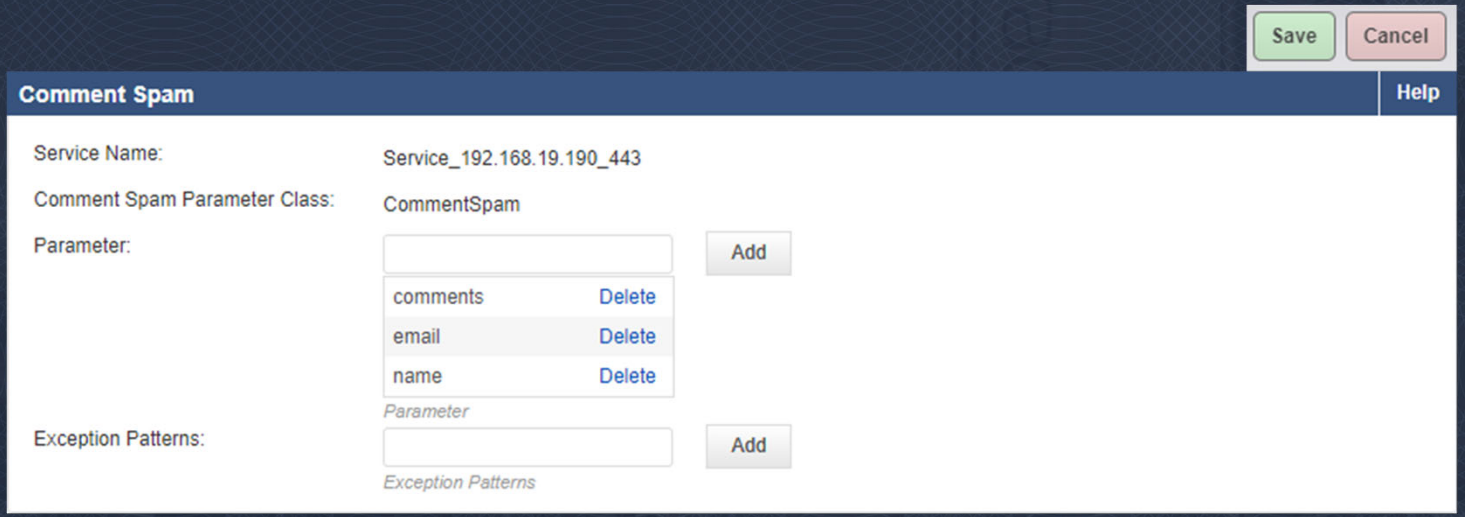
Comment Spam: Add the parameters



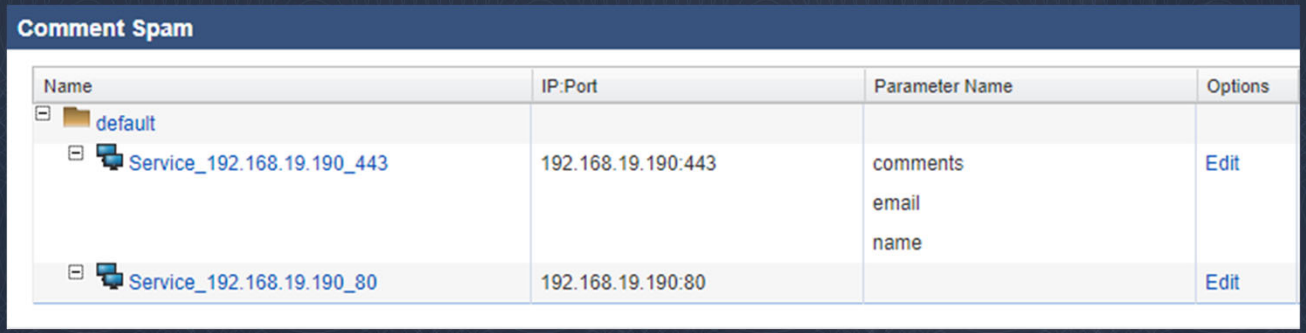
Comment Spam: Add the parameters



Comment Spam: Save the policy



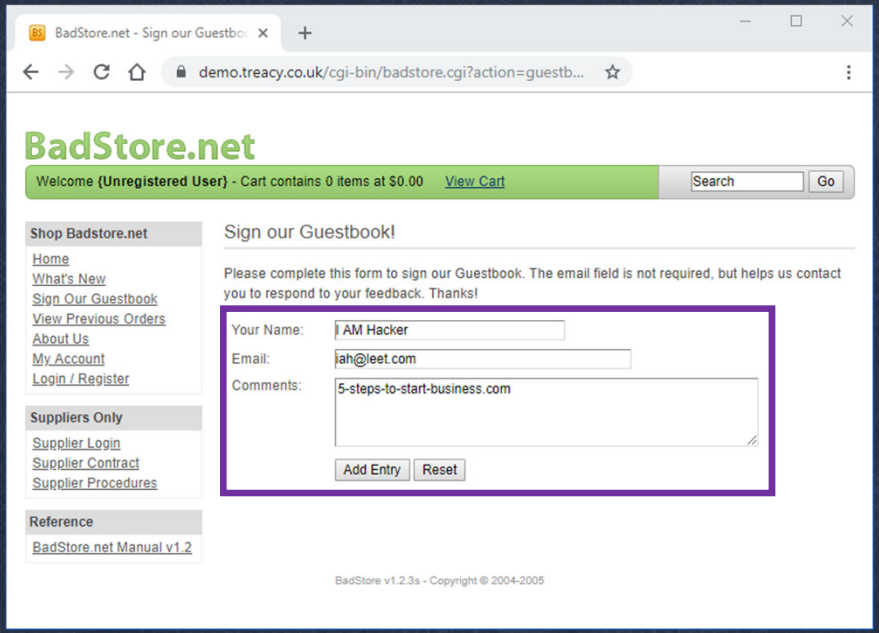
Comment Spam: Policy



Comment Spam

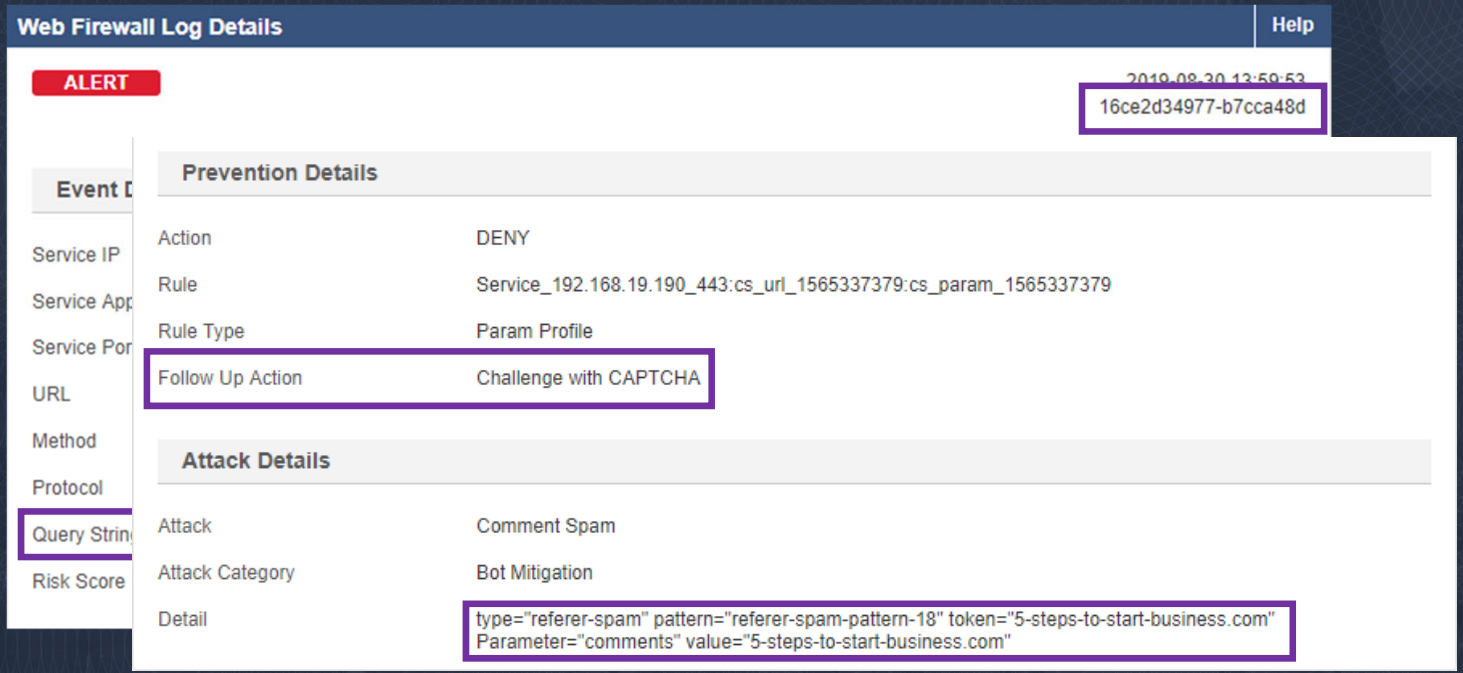
Name	IP:Port	Parameter Name	Options
default			
Service_192.168.19.190_443	192.168.19.190:443	comments email name	Edit
Service_192.168.19.190_80	192.168.19.190:80		Edit

Testing using the comment spam link



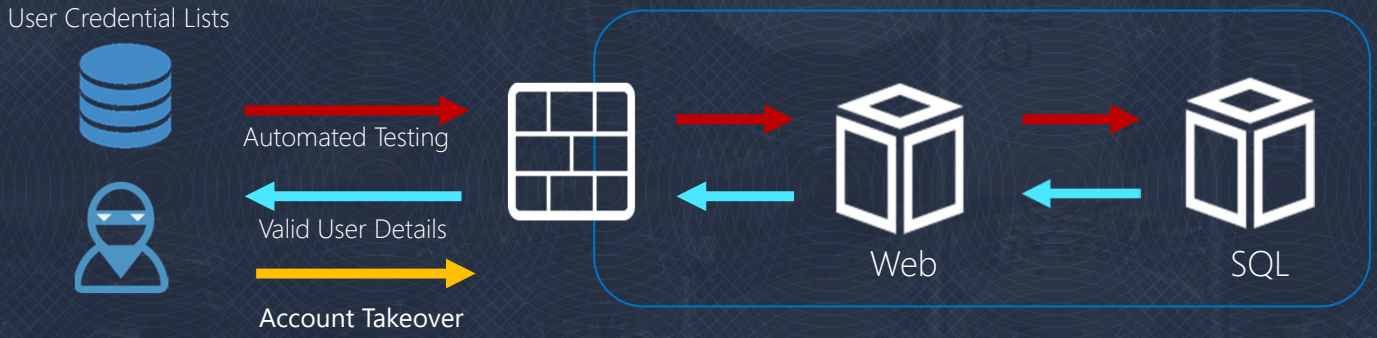
WAF blocks with…

WAF Logs…

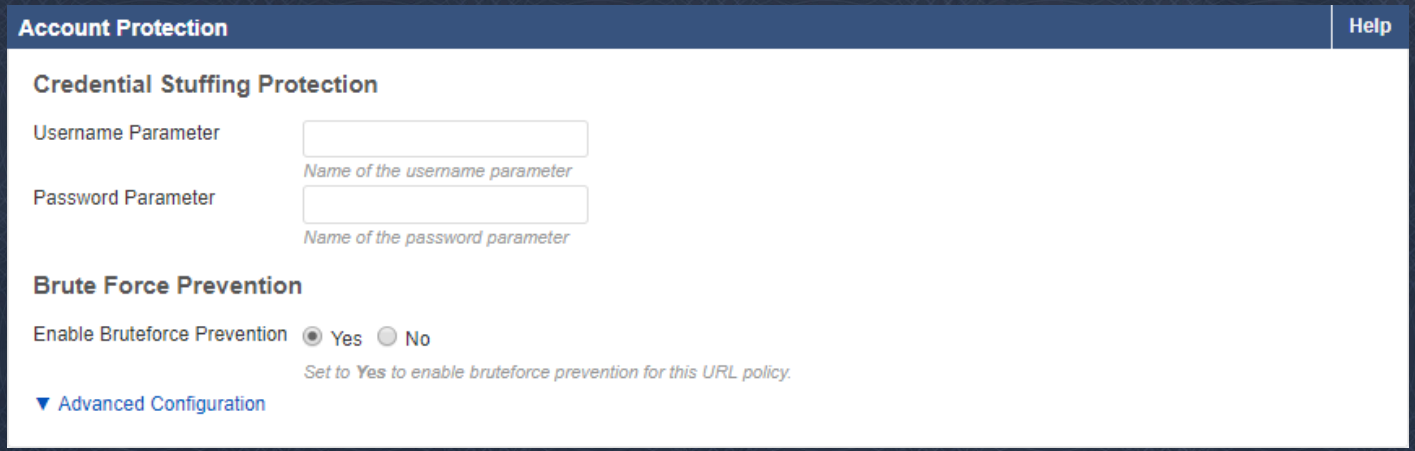

Web Firewall Log Details
Help
ALERT
16ce2d34977-b7cca48d
Event D
Service IP
Service App
Service Por
URL
Method
Protocol
Query Strin
Risk Score
Prevention Details
Action
DENY
Rule
Service_192.168.19.190_443:cs_url_1565337379:cs_param_1565337379
Rule Type
Param Profile
Follow Up Action
Challenge with CAPTCHA
Attack Details
Attack
Comment Spam
Attack Category
Bot Mitigation
Detail
type="referer-spam" pattern="referer-spam-pattern-18" token="5-steps-to-start-business.com"
Parameter="comments" value="5-steps-to-start-business.com"

Credential stuffing

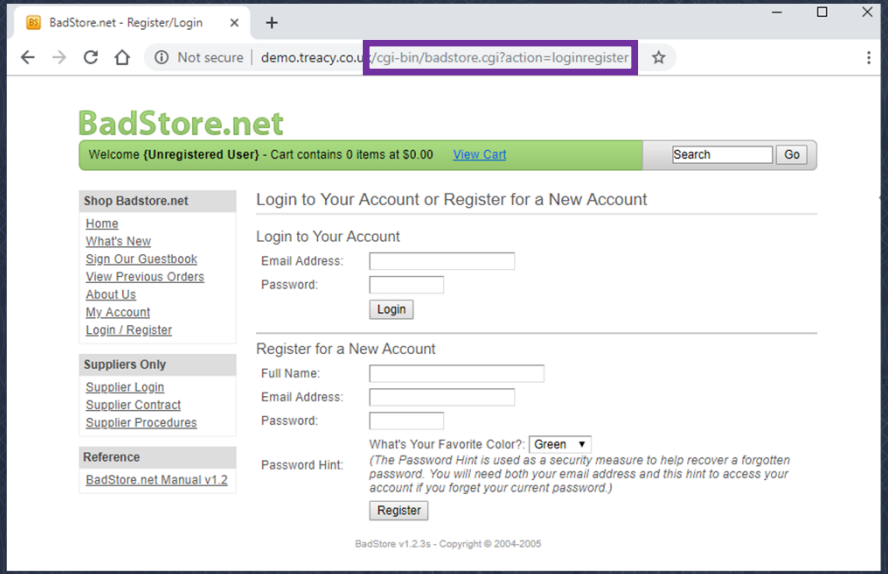
Lists of authentication credentials stolen from elsewhere are tested against the application's authentication mechanisms to identify whether users have re-used the same login credentials



Credential stuffing demo

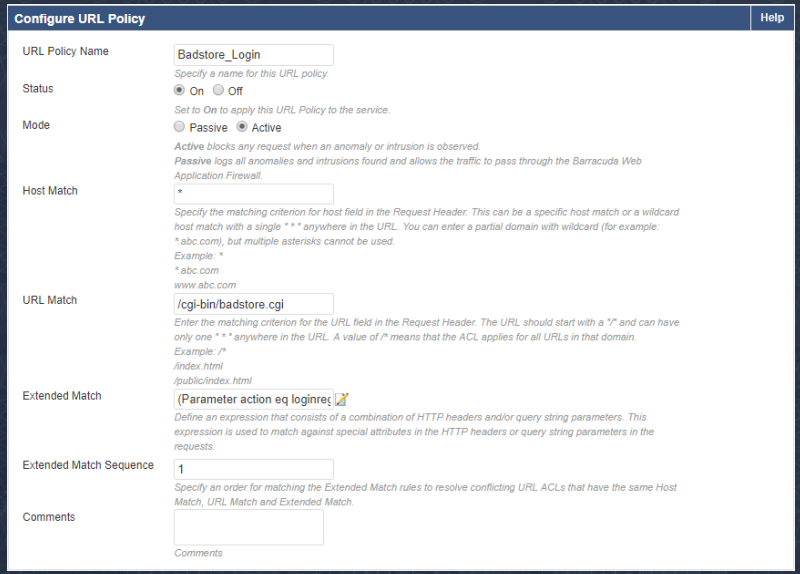


What is the URL we are going to protect?

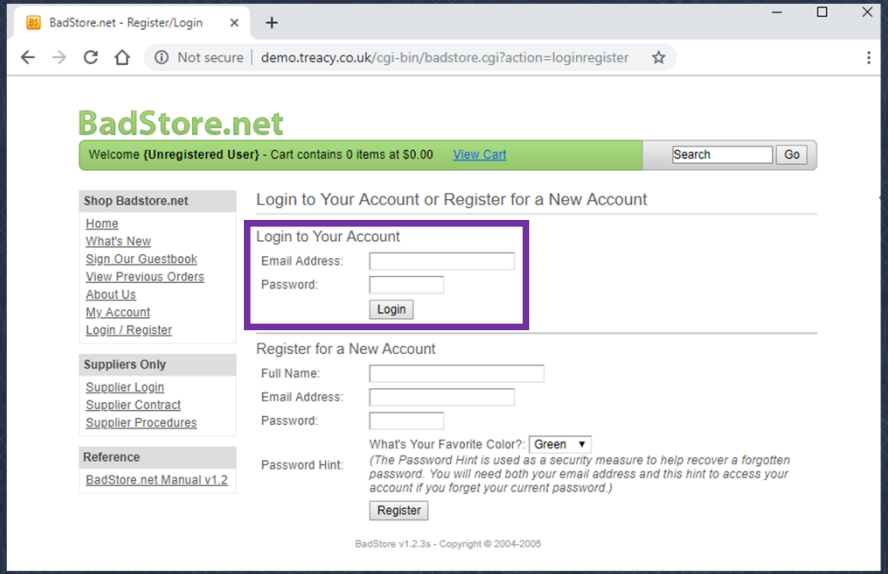


Bot Mitigation Policy: Configure URL Policy

Bot Mitigation Policy: Configure URL Policy

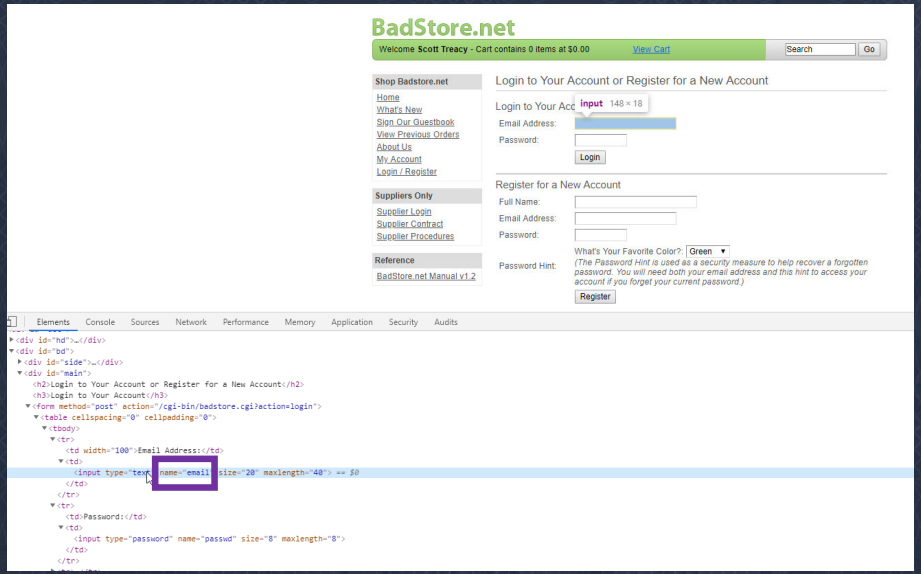


What are the login parameters?

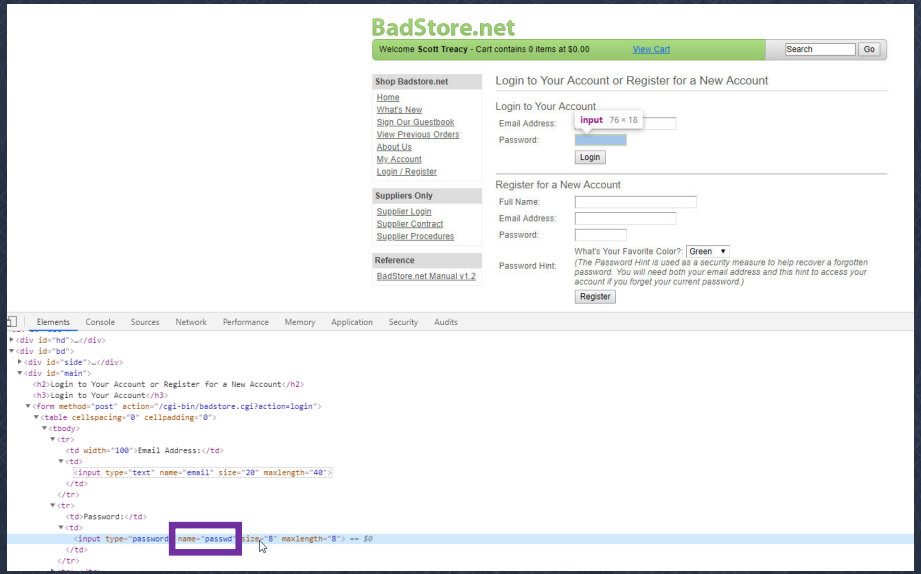


Bot Mitigation Policy: Account Protection

What is the Username Parameter name?

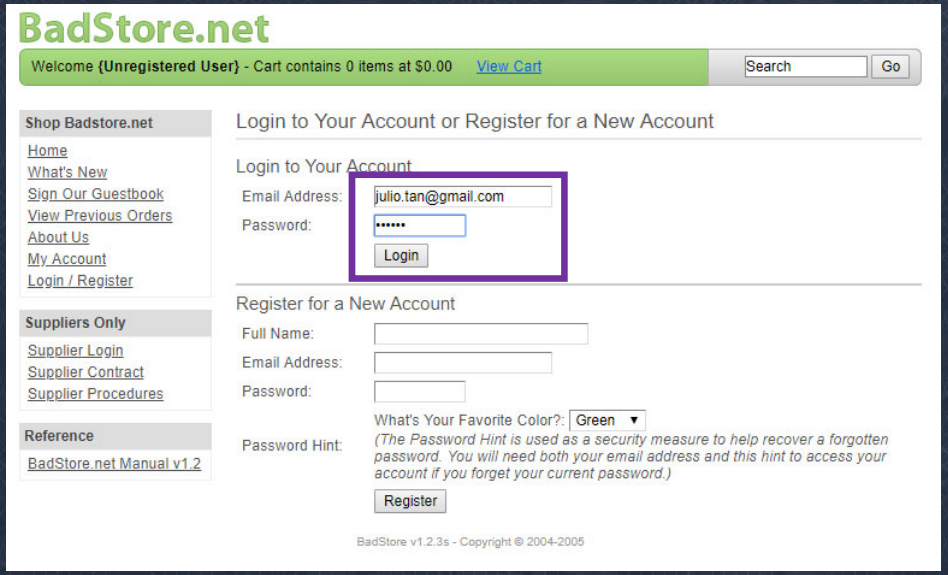


What is the Password Parameter name?

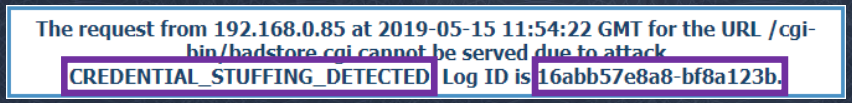


Bot Mitigation Policy: Account Protection

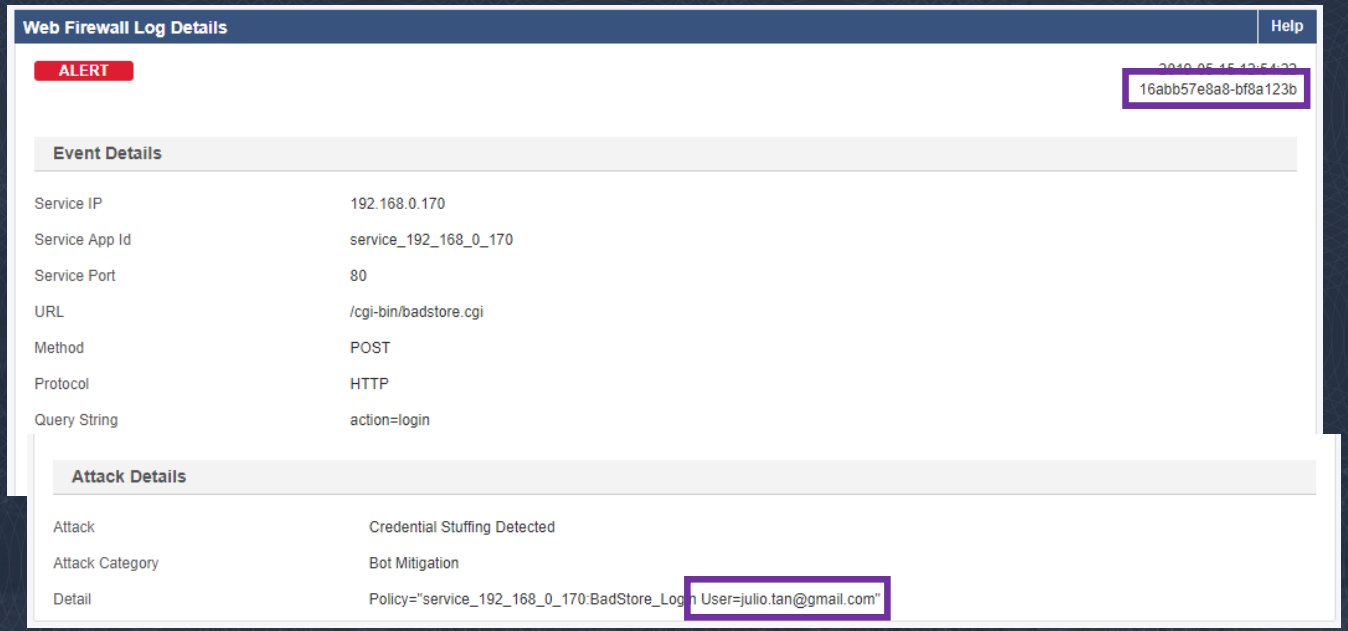
Testing some compromised user credentials



WAF blocks with…



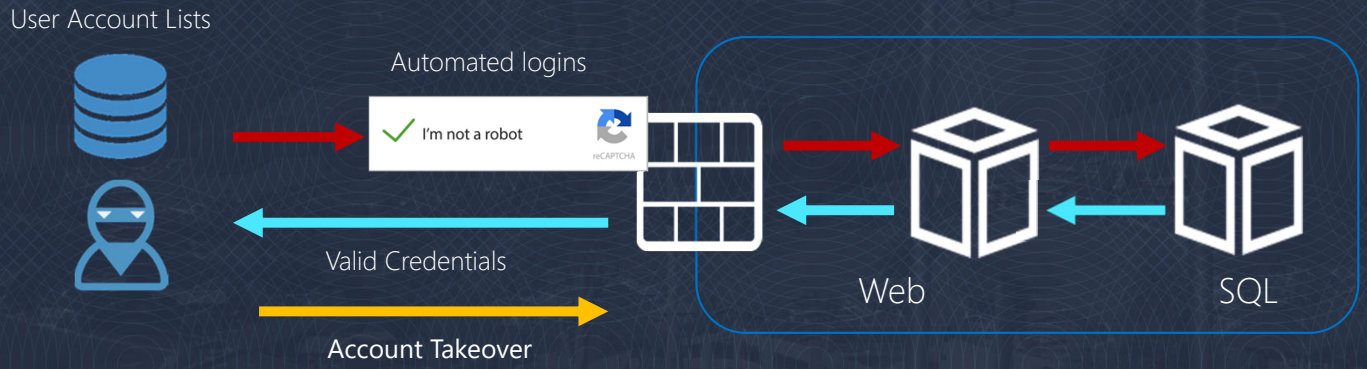
WAF logs…


Web Firewall Log Details
Help
ALERT
16abb57e8a8-bf8a123b
Event Details
Service IP
192.168.0.170
Service App Id
service_192_168_0_170
Service Port
80
URL
/cgi-bin/badstore.cgi
Method
POST
Protocol
HTTP
Query String
action=login
Attack Details
Attack
Credential Stuffing Detected
Attack Category
Bot Mitigation
Detail
Policy="service_192_168_0_170:BadStore_Login User=julio.tan@gmail.com"

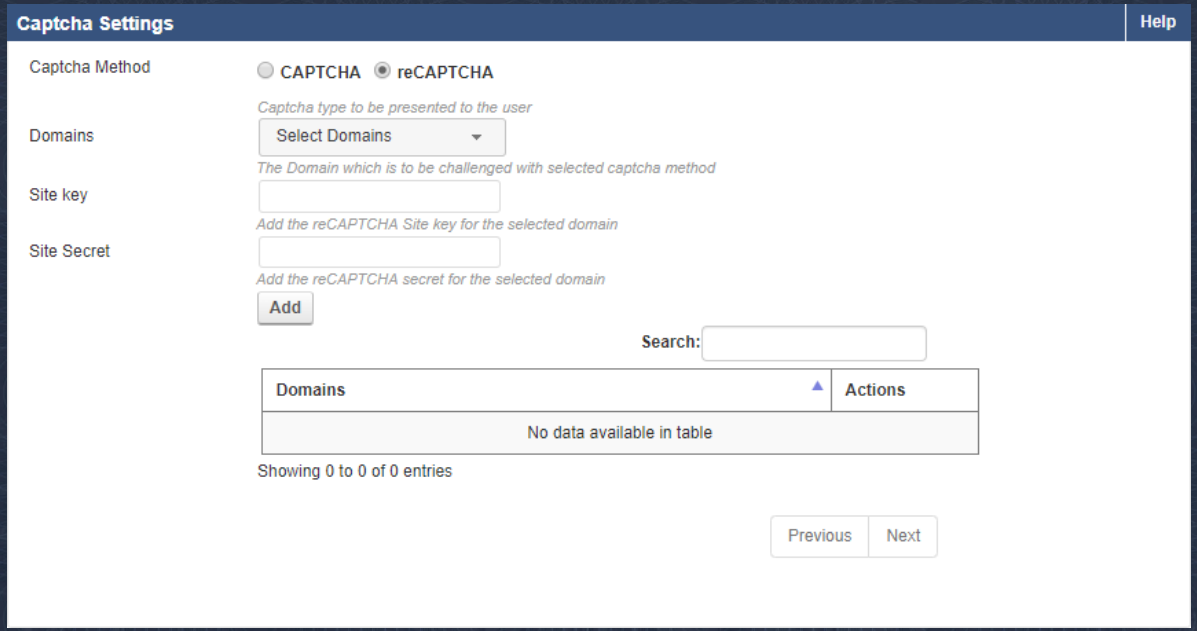
Credential cracking (With CAPTCHA defeat)

Identify valid login credentials by trying different values for usernames and/or passwords.

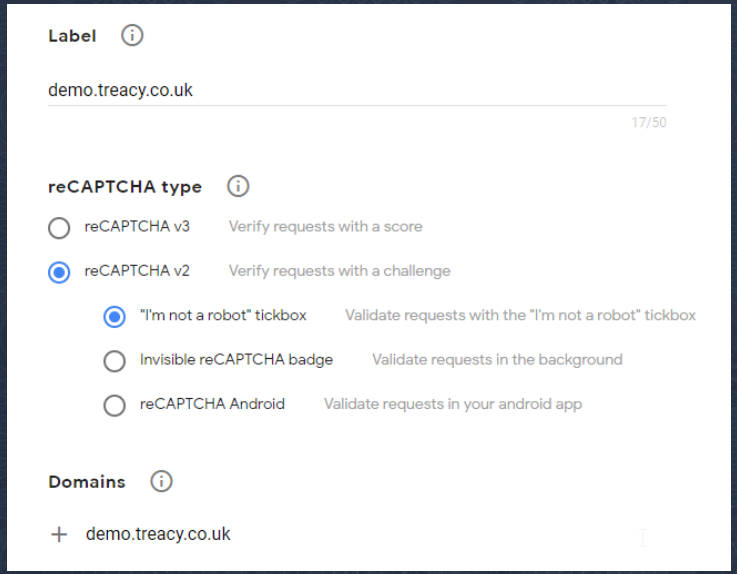
Additional automation required to defeat CAPTCHA



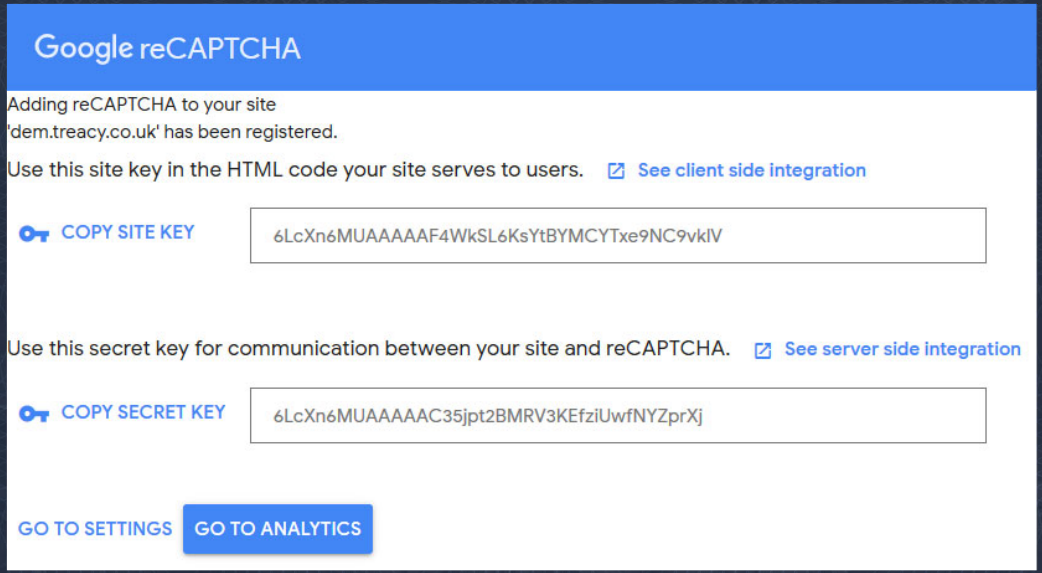
reCAPTCHA demo



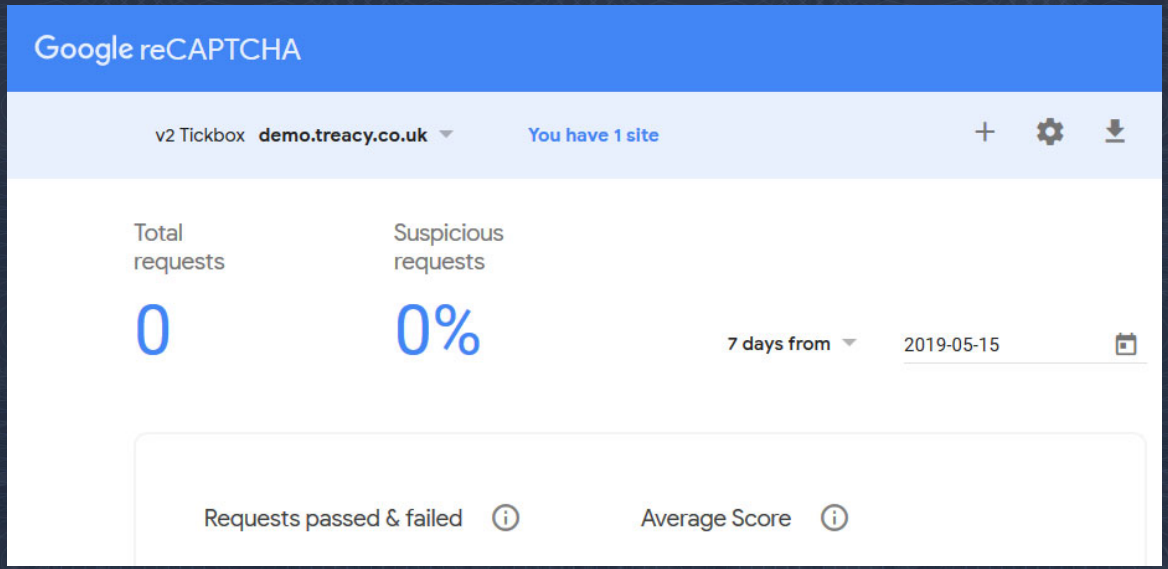
Google reCAPTCHA settings: Create Domain



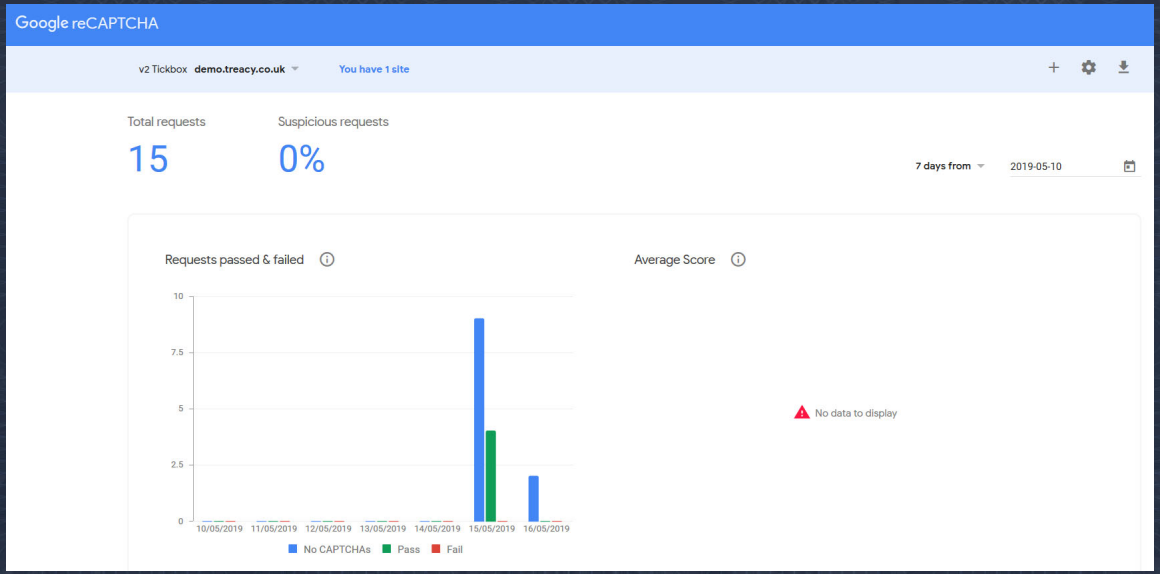
Google reCAPTCHA settings: Keys



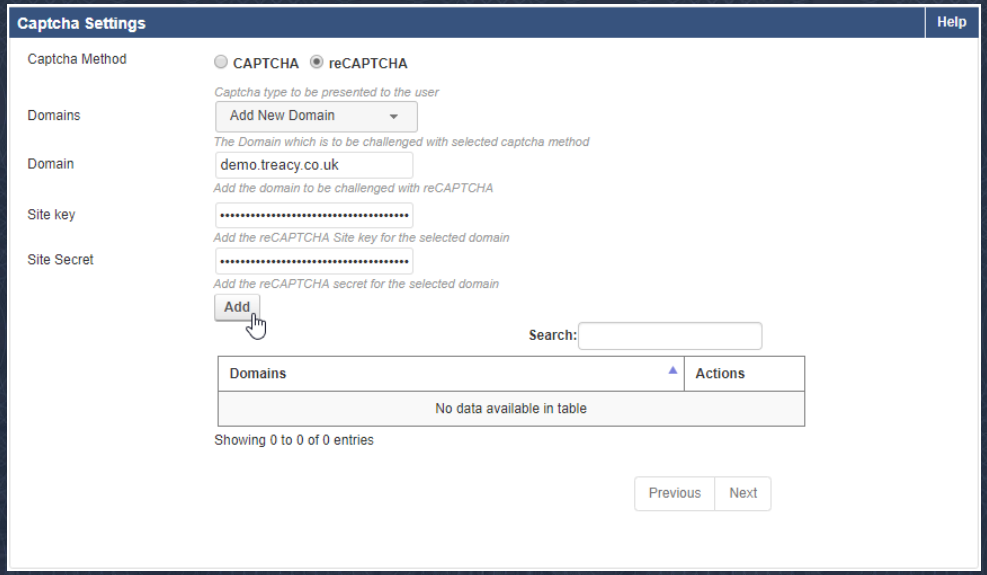
Google reCAPTCHA settings: Domain Admin



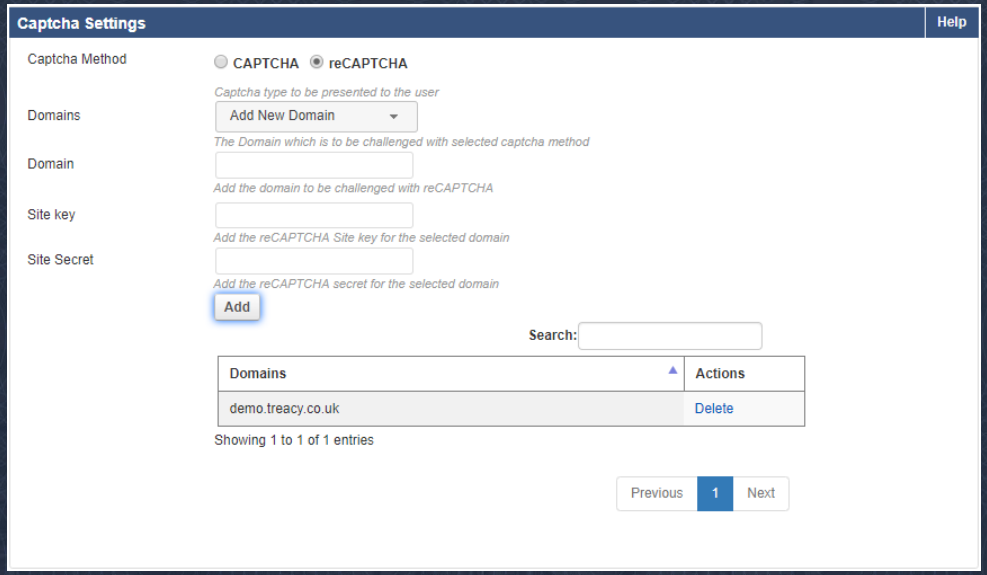
Google reCAPTCHA settings: Domain Admin



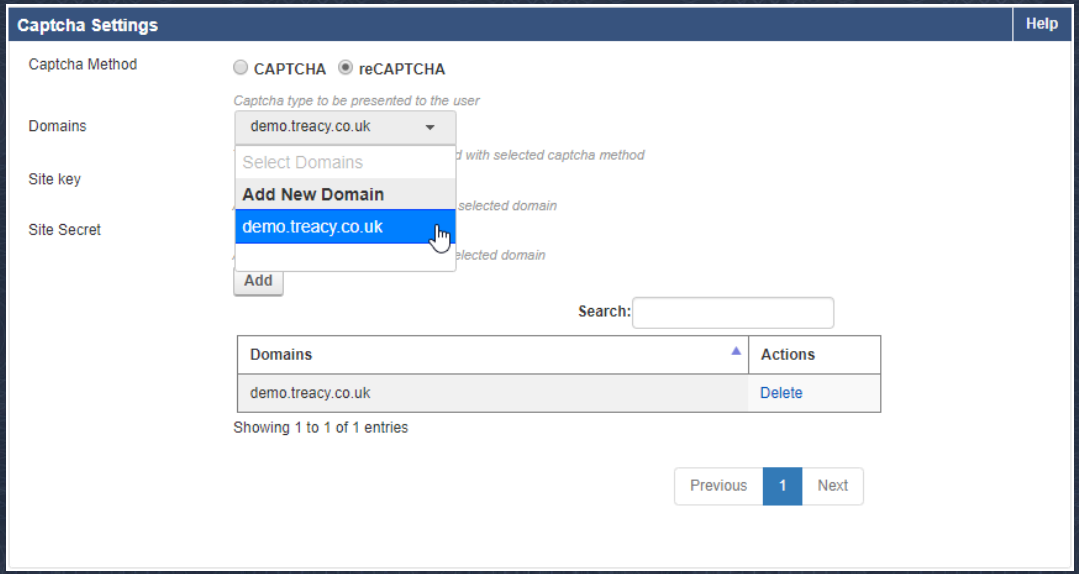
Barracuda WAF reCAPTCHA Service Settings



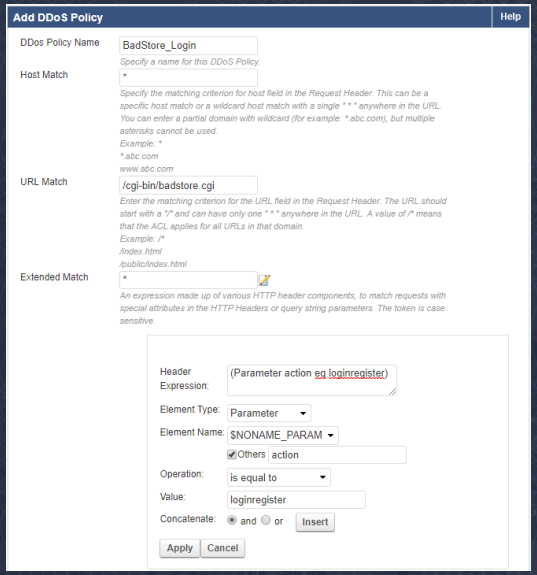
Barracuda WAF reCAPTCHA Service Settings



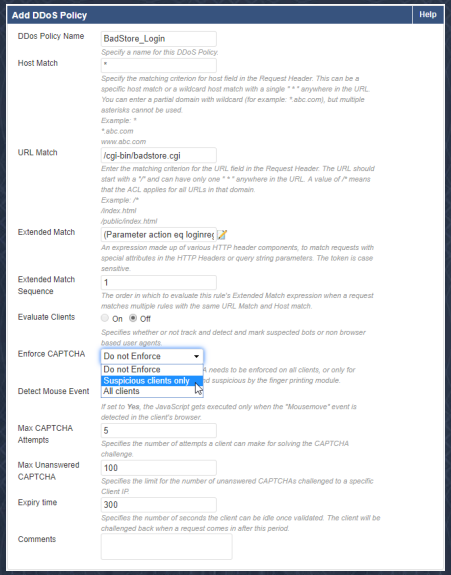
Barracuda WAF reCAPTCHA Service Settings



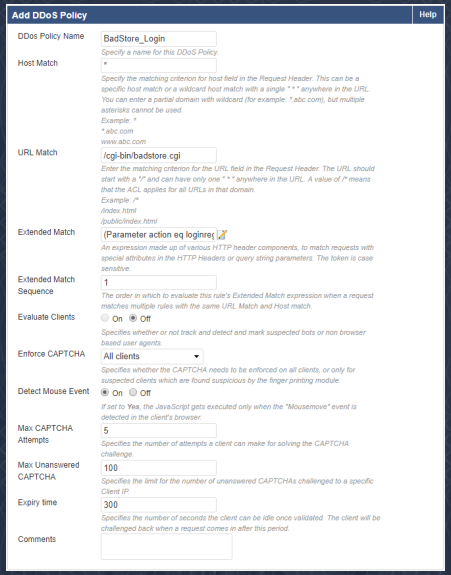
Barracuda WAF DDoS Policy CAPTCHA settings



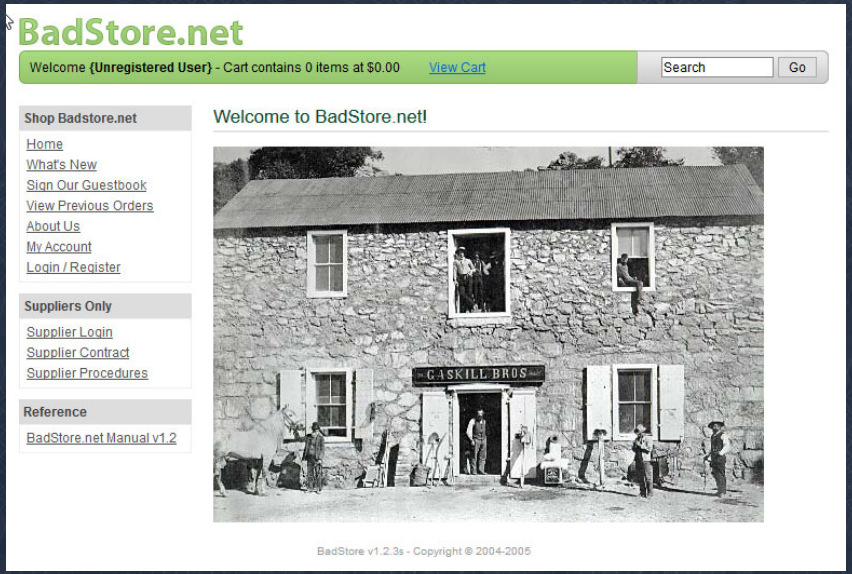
Barracuda WAF DDoS Policy CAPTCHA settings



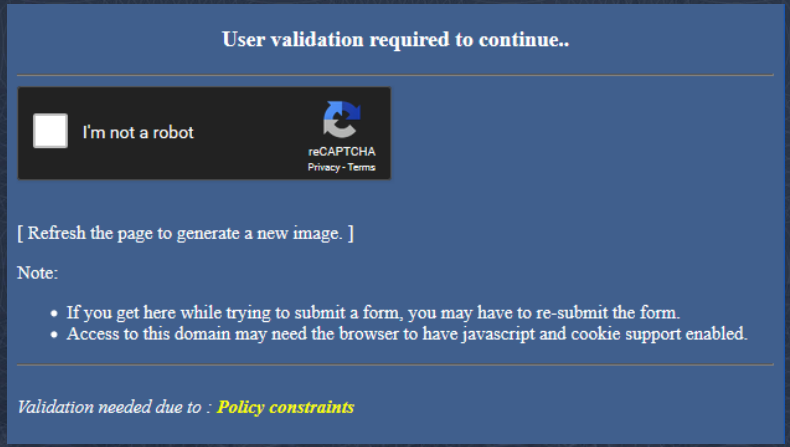
Barracuda WAF DDoS Policy CAPTCHA settings



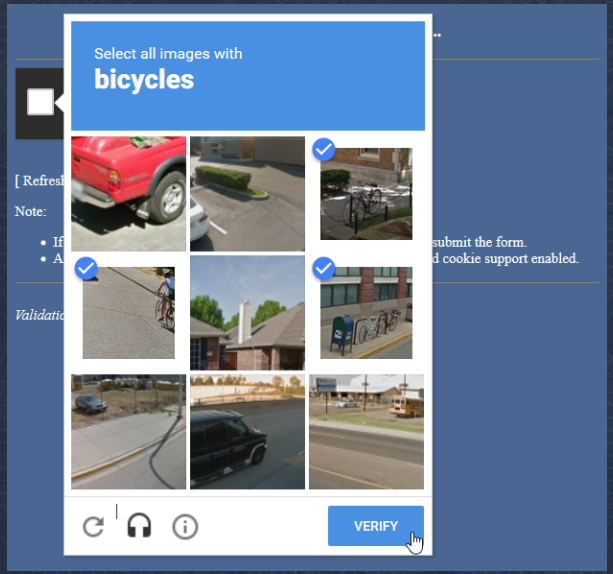
The BadStore… Lets Login!



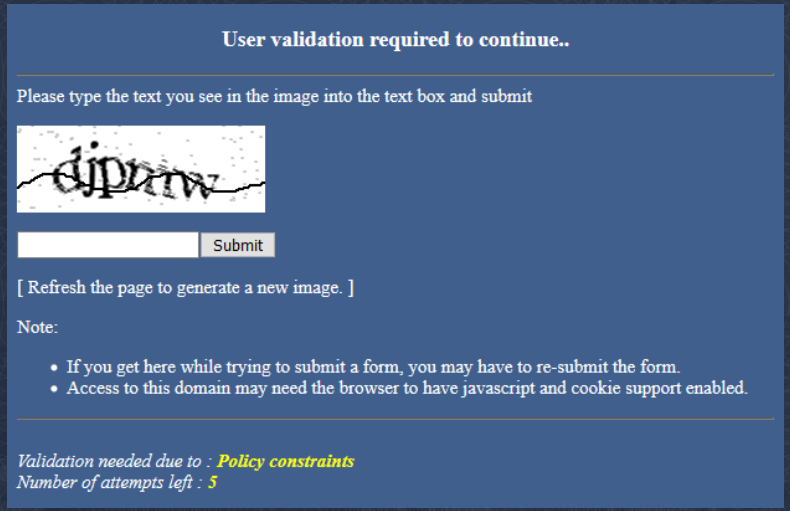
Barracuda WAF inserts the reCAPTCHA…



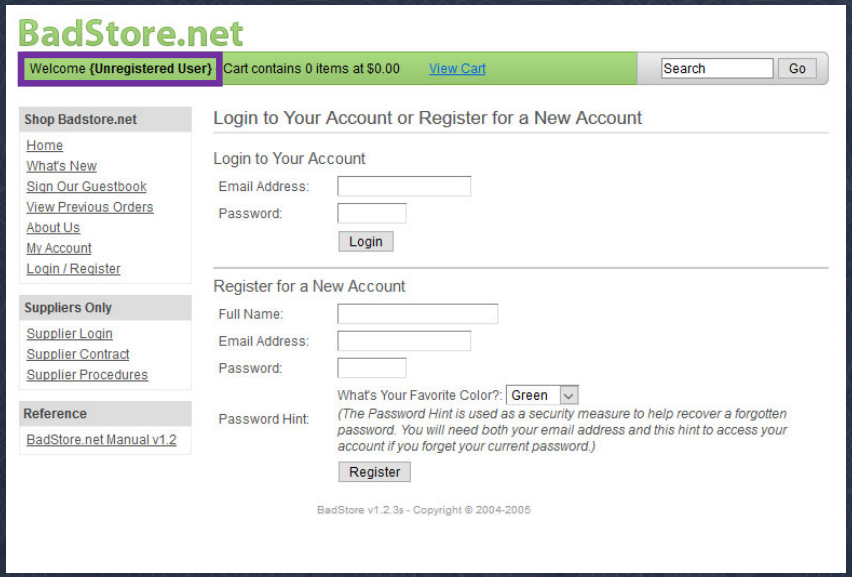
reCAPTCHA verify (if Google are suspicious)…



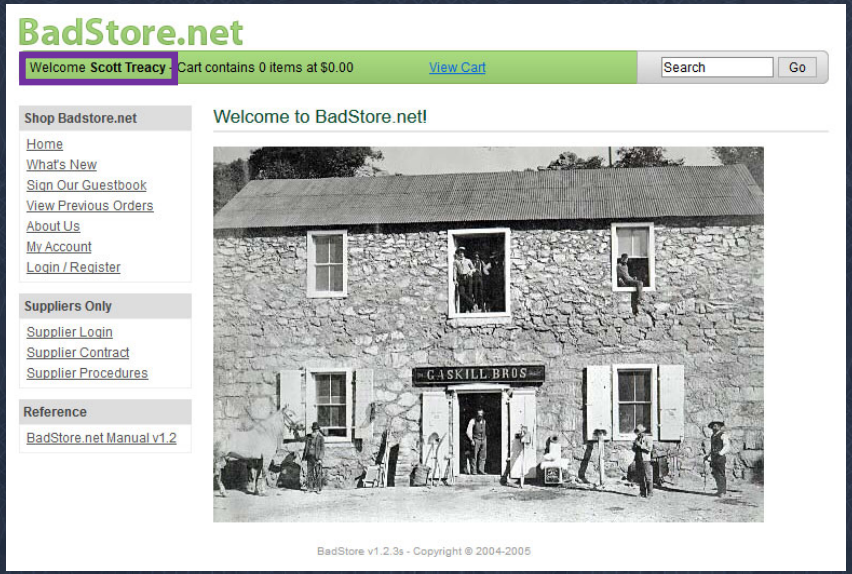
Barracuda WAF falls back to internal CAPTCHA if there is reCAPTCHA issue…



You successfully proved you are Human! Now you can access the Login…



…and now Logged in



Q&A

We're here to help…

Try out the Advance Bot Protection trial

Check out the bot protection SKUs and Price Information

Want to know more about WAF and WAF-as-a-Service?

- I can come and talk to your teams about Application Security
- I can help with your Evaluations and PoC's
- Email: REDACTED
- Twitter: REDACTED

Or, contact the Barracuda EMEA Consulting Solutions Team

REDACTED


Thank you
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT