



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

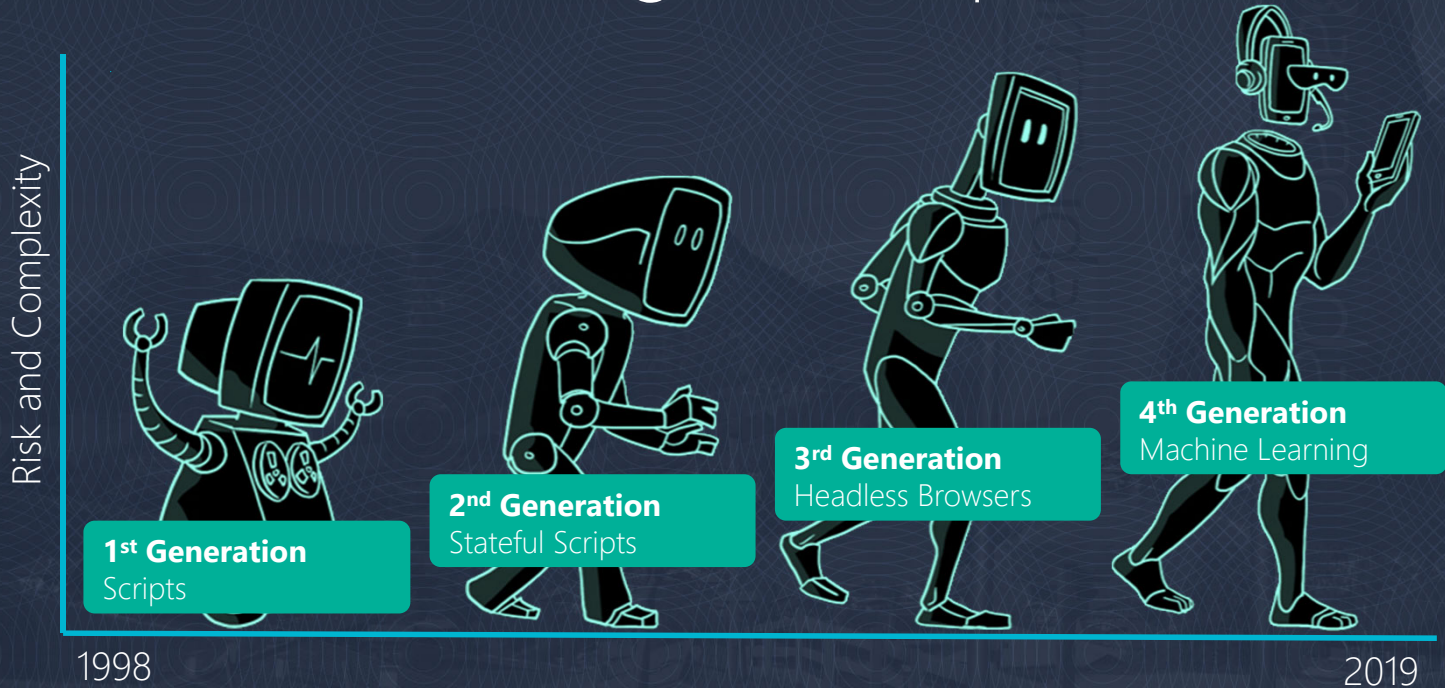
Closing plus Q&A



A VERY Short History of Bots



Bots are becoming more sophisticated



Vulnerabilities are being exploited !

Forbes

13,559 views | Sep 9, 2018, 01:00pm

380,000 Passengers Affected By 'Malicious' British Airways Hack

The New York Times

Marriott Hacking Exposes Data of Up to 500 Million Guests

ars TECHNICA

BIZ & IT —

Failure to patch two-month-old bug led to massive Equifax breach

Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers.

DAN GOODIN - 9/14/2017, 4:12 AM



Vulnerabilities are being exploited !



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](#)

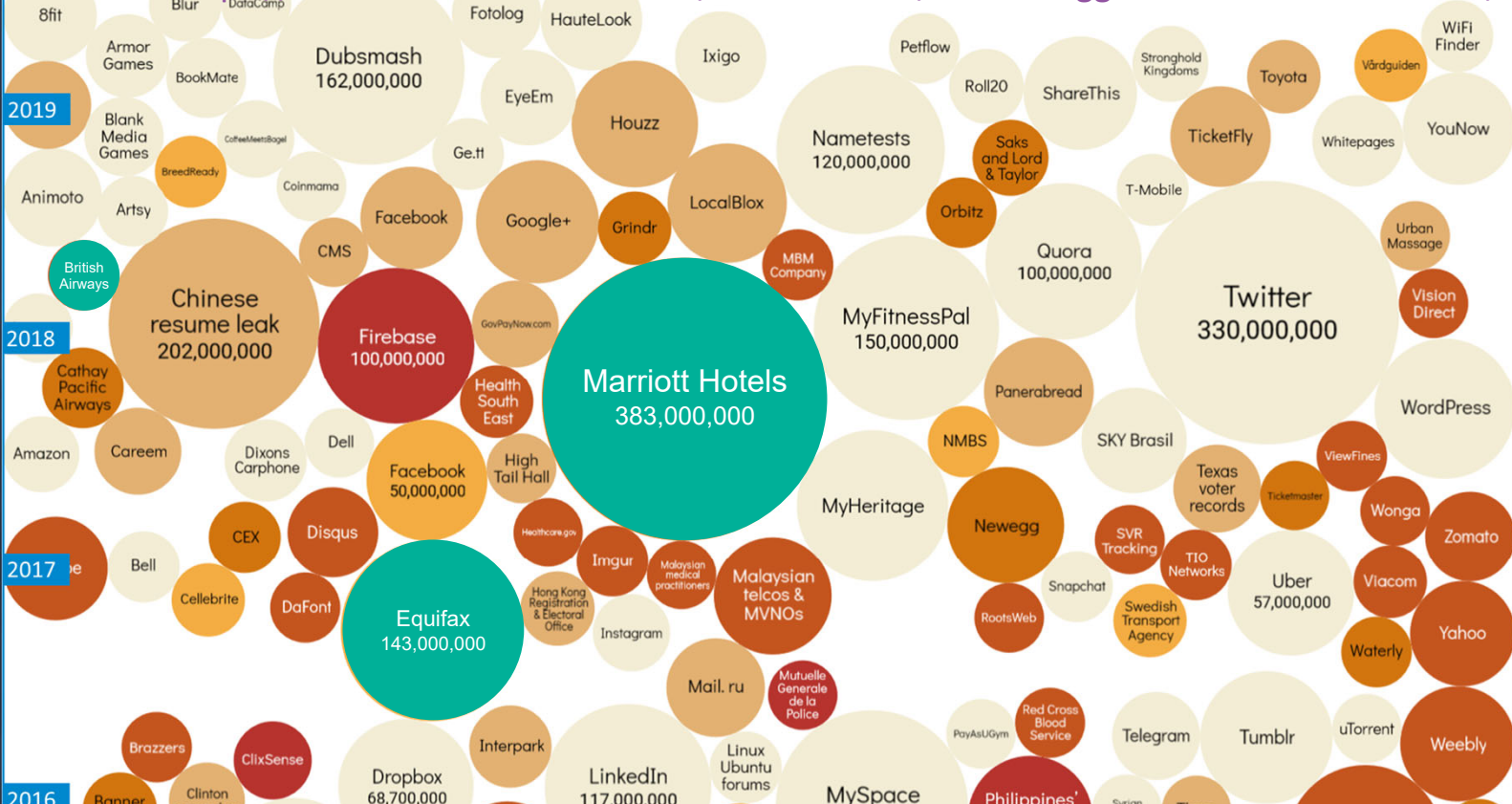
July 9, 2019, 3:14 PM GMT+1

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



<https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



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

BASICSECURITY POLICIESWEBSITESBOT MITIGATIONACCESS CONTROLNETWORKSADVANCED

Search help topics

Bot MitigationBot Spam MitigationApplication DDoS MitigationLibraries

Filterdefault

Bot Mitigation Policy

PreferencesHelp

Name	URL Policy	Status	Bot Detection	Account Protection	File Upload Security	Data Theft ...	Options			
default										
test (192.168.0.152:80)							Add			
Host Match: * URL Match: /*	Policy Name: default-url-... Rate Control Pool: NONE	Statu... Mode...	Web Scra...	Brute Force Preve... Credential Stuffing ...	Anti-virus: On BATP Scan: On	On	Edit	Copy	Rename	Delete

Web Scraping Policies

Add PolicyHelp

Policy Name	Insert Hidden Links	Insert Disallowed URLs	Insert JavaScript	Insert Delay	Delay Time			
test	Yes	Yes	Yes	Yes	10	Edit	Delete	

Session Tracking

PreferencesHelp

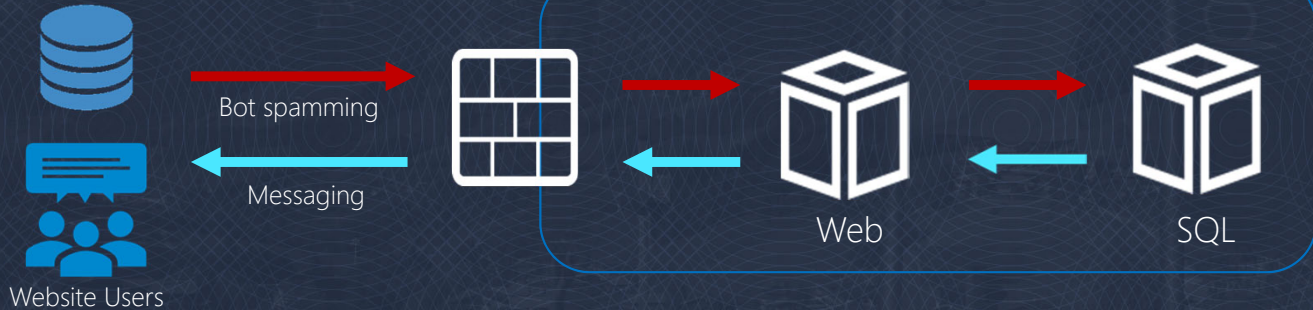
Name	IP:Port	Session Identifiers	New Session Count	Interval	Status	Options	
default							
test	192.168.0.152:80	PHPSESSID-session		60	On	Edit	



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 Database



Comment Spam demo

Comment Spam

[Help](#)

Service Name: Service_192.168.19.190_443

Comment Spam Parameter Class: CommentSpam

Parameter:

Add

Parameter

Exception Patterns:

Add

Exception Patterns



The Comment Spam Database

Spam URL List

[View Spam URL List](#)

List of all the referer entries against which WAF provides protection



View the 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



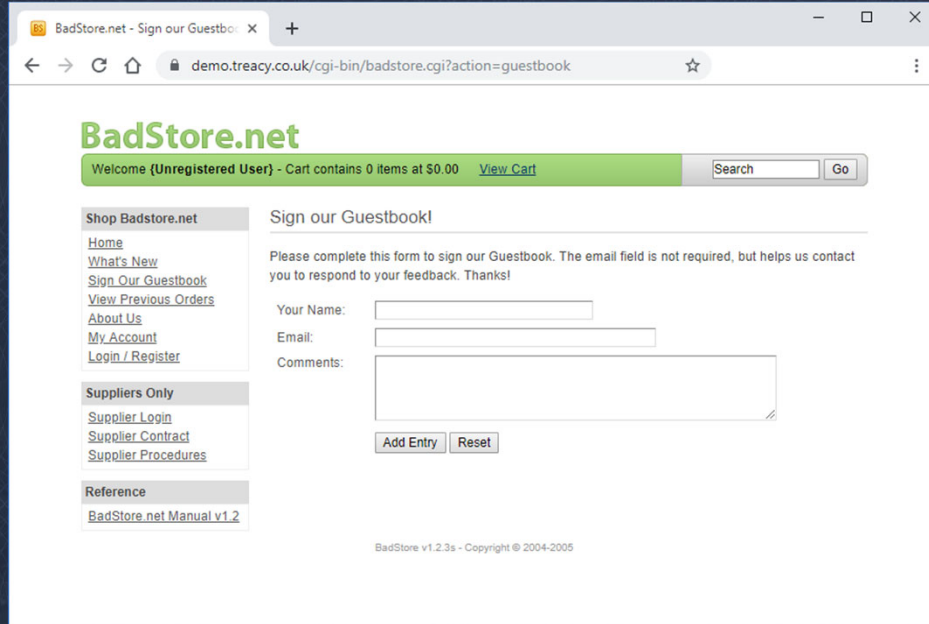
Pick a Spam URL to test with

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?



The screenshot shows a web browser window with the address bar displaying "demo.treacy.co.uk/cgi-bin/badstore.cgi?action=guestbook". The page title is "BadStore.net" and the main heading is "Sign our Guestbook!". The page content includes a welcome message for an unregistered user, a search bar, and a sign-in form with fields for "Your Name:", "Email:", and "Comments:". The form also has "Add Entry" and "Reset" buttons. A left sidebar contains navigation links for "Shop Badstore.net", "Suppliers Only", and "Reference".

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#)

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contract](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name:

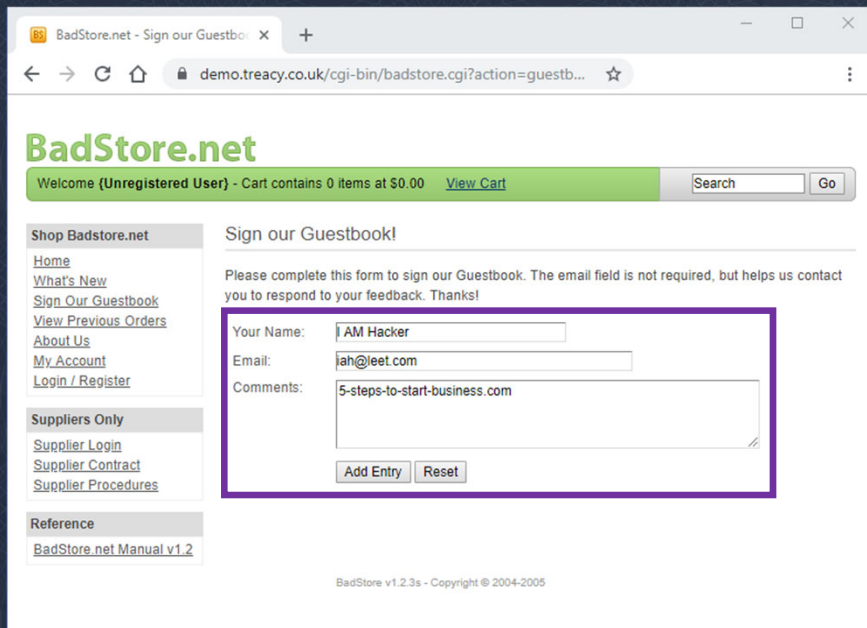
Email:

Comments:

BadStore v1.2.3s - Copyright © 2004-2005



Testing using the comment spam URL



BadStore.net - Sign our Guestbook

demo.treacy.co.uk/cgi-bin/badstore.cgi?action=guestb...

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#) Search Go

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contract](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name:

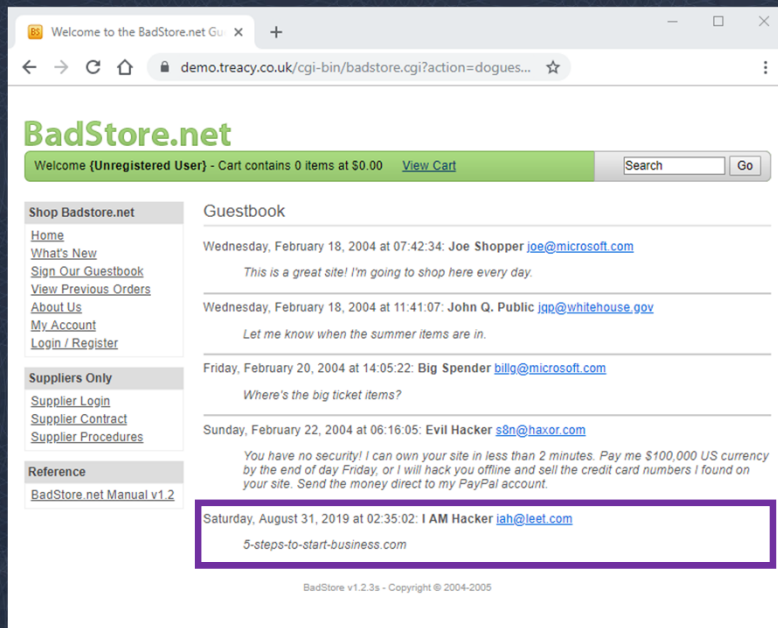
Email:

Comments:

BadStore v1.2.3s - Copyright © 2004-2005



The BadStore Guestbook displays the Spam URL



Comment Spam Parameters

Comment Spam

[Help](#)

Service Name: Service_192.168.19.190_443

Comment Spam Parameter Class: CommentSpam

Parameter:

Add

Parameter

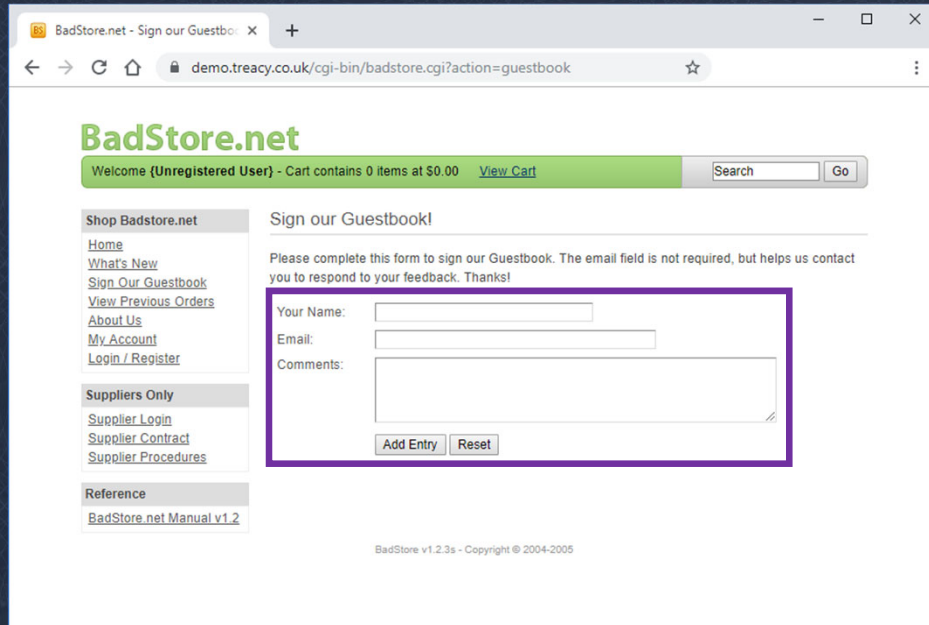
Exception Patterns:

Add

Exception Patterns



What are the comment field parameters?



BadStore.net - Sign our Guestbook

demo.treacy.co.uk/cgi-bin/badstore.cgi?action=guestbook

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#)

Search

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contract](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name:

Email:

Comments:

BadStore v1.2.3s - Copyright © 2004-2005



What is the Name parameter called?

The screenshot displays the BadStore.net website interface. At the top, a green banner reads "Welcome (Unregistered User) - Cart contains 0 items at \$0.00" with a "View Cart" link. A search bar is located to the right. The main content area is divided into a left sidebar with navigation links (Home, What's New, Sign Our Guestbook, View Previous Orders, About Us, My Account, Login / Register) and a right section titled "Sign our Guestbook!". The guestbook section includes a message: "Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to" followed by a red "input" tooltip pointing to a text field labeled "Your Name:". Below this are fields for "Email:" and "Comments:". At the bottom of the form are "Add Entry" and "Reset" buttons. The footer indicates "BadStore v1.2.3s - Copyright © 2004-2005".

Below the website screenshot, the browser's developer tools are open to the "Elements" tab. The DOM tree shows the HTML structure of the form. The following code is visible:

```
<form method="POST" action="/cgi-bin/badstore.cgi?action=doguestbook" enctype="application/x-www-form-urlencoded"></form>
<tbody>
  <tr>
    <td>Your Name:</td>
    <td>
      <input type="text" name="name" size="30" == $0
    </td>
  </tr>
  <tr>
    <td>Email:</td>
    <td>
      <input type="text"
    </td>
  </tr>
  <tr>
    <td>Comments:</td>
    <td>
      <input type="text"
    </td>
  </tr>
  <tr>
    <td colspan="2">
      <input type="button" value="Add Entry" />
      <input type="button" value="Reset" />
    </td>
  </tr>
</tbody>
```

The "name" attribute in the `<input type="text" name="name" size="30" == $0` line is highlighted with a red box, and a mouse cursor points to it.



What is the Email parameter called?

The screenshot displays the BadStore.net website interface. At the top, a green banner reads "Welcome (Unregistered User) - Cart contains 0 items at \$0.00" with a "View Cart" link. A search bar is located to the right. The left sidebar contains navigation links under "Shop Badstore.net" (Home, What's New, Sign Our Guestbook, View Previous Orders, About Us, My Account, Login / Register), "Suppliers Only" (Supplier Login, Supplier Contract, Supplier Procedures), and "Reference" (BadStore.net Manual v1.2). The main content area is titled "Sign our Guestbook!" and includes instructions: "Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!". The form has three fields: "Your Name:" (with a tooltip showing "input 268 x 18"), "Email:" (highlighted with a blue box), and "Comments:". "Add Entry" and "Reset" buttons are at the bottom of the form. Below the website content, the browser's developer tools are open to the "Elements" tab, showing the HTML structure. The email input field is highlighted with a purple box, and its attributes are visible in the code: `<input type="text" name="email" size="40">`. The tooltip for the name field also points to this line of code.

BadStore.net

Welcome (Unregistered User) - Cart contains 0 items at \$0.00 [View Cart](#)

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contract](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name: input 268 x 18

Email:

Comments:

BadStore v1.2.3s - Copyright © 2004-2005

Elements Console Sources Network Performance Memory Application Security Audits

```
<form method="POST" action="/cgi-bin/badstore.cgi?action=doguestbook" enctype="application/x-www-form-urlencoded"></form>
<tbody>
  <tr></tr>
  <tr>
    <td>Email:</td>
    <td>
      <input type="text" name="email" size="40">
    </td>
  </tr>
  <tr></tr>
</tbody>
```



What is the Comments parameter called?

The screenshot displays the BadStore.net website interface. At the top, the site name "BadStore.net" is in green. Below it, a green banner reads "Welcome (Unregistered User) - Cart contains 0 items at \$0.00" with a "View Cart" link. A search bar with a "Go" button is on the right. The left sidebar contains navigation links under "Shop Badstore.net" (Home, What's New, Sign Our Guestbook, View Previous Orders, About Us, My Account, Login / Register), "Suppliers Only" (Supplier Login, Supplier Contract, Supplier Procedures), and "Reference" (BadStore.net Manual v1.2). The main content area is titled "Sign our Guestbook!" and includes instructions: "Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!". The form has three fields: "Your Name:" (text input), "Email:" (text input with a tooltip saying "textarea 383 x 62"), and "Comments:" (a large blue text area). Below the form are "Add Entry" and "Reset" buttons. At the bottom of the page, it says "BadStore v1.2.3s - Copyright © 2004-2005".

Below the website screenshot, the HTML source code is shown in a developer tool. The code is for a form with method="POST" and action="/cgi-bin/badstore.cgi?action=doguestbook". The form body contains three rows. The third row is for comments, with a text area element highlighted by a purple box. The HTML for the text area is:

```
<td valign="TOP">Comments:</td>
<td>
<textarea name="comments" cols="60" rows="4"></textarea> == $0
</td>
</tr>
```



Comment Spam: Add the parameters

Comment Spam		Help
Service Name:	Service_192.168.19.190_443	
Comment Spam Parameter Class:	CommentSpam	
Parameter:	<input type="text" value="comments"/>	<input type="button" value="Add"/>
	<i>Parameter</i>	
Exception Patterns:	<input type="text"/>	<input type="button" value="Add"/>
	<i>Exception Patterns</i>	



Comment Spam: Add the parameters

Comment Spam

Help

Service Name:

Service_192.168.19.190_443

Comment Spam Parameter Class:

CommentSpam

Parameter:

email

comments

Delete

Add

Exception Patterns:

Add

Parameter

Exception Patterns



Comment Spam: Add the parameters

Comment Spam

Help

Service Name:

Service_192.168.19.190_443

Comment Spam Parameter Class:

CommentSpam

Parameter:

name	
comments	Delete
email	Delete

Parameter

Exception Patterns

Add

Add



Comment Spam: Save the policy

Save

Cancel

Comment Spam

Help

Service Name: Service_192.168.19.190_443

Comment Spam Parameter Class: CommentSpam

Parameter:

Add

comments [Delete](#)

email [Delete](#)

name [Delete](#)

Parameter

Exception Patterns:




Add

Exception Patterns



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

The screenshot shows a web browser window with the address bar displaying `demo.treacy.co.uk/cgi-bin/badstore.cgi?action=guestb...`. The page title is "BadStore.net - Sign our Guestbook". The main heading is "BadStore.net" in green. Below it, a green banner says "Welcome {Unregistered User} - Cart contains 0 items at \$0.00" with a "View Cart" link. A search bar is on the right. The left sidebar has links for "Shop Badstore.net" (Home, What's New, Sign Our Guestbook, View Previous Orders, About Us, My Account, Login / Register), "Suppliers Only" (Supplier Login, Supplier Contract, Supplier Procedures), and "Reference" (BadStore.net Manual v1.2). The main content area is titled "Sign our Guestbook!" and contains a form with the following fields: "Your Name:" (filled with "I AM Hacker"), "Email:" (filled with "jah@leet.com"), and "Comments:" (filled with "5-steps-to-start-business.com"). The "Comments:" field is highlighted with a purple border. Below the form are "Add Entry" and "Reset" buttons. The footer says "BadStore v1.2.3s - Copyright © 2004-2005".

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#)

Search

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contract](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name:

Email:

Comments:

BadStore v1.2.3s - Copyright © 2004-2005



WAF blocks with...

The request from 192.168.19.42 at 2019-08-30 13:59:53 GMT for the URL /cgi-bin/badstore.cgi cannot be served due to attack COMMENT_SPAM Log ID is 16ce2d34977-b7cca48d.



WAF Logs...

Web Firewall Log Details

[Help](#)**ALERT**

2010-08-30 13:50:53

16ce2d34977-b7cca48d

Event Details**Prevention Details**

Service IP	Action	DENY
Service App	Rule	Service_192.168.19.190_443:cs_url_1565337379:cs_param_1565337379
Service Port	Rule Type	Param Profile
URL	Follow Up Action	Challenge with CAPTCHA

Method

Protocol

Query String

Risk Score

Attack Details

Attack	Comment Spam
Attack Category	Bot Mitigation
Detail	type="referrer-spam" pattern="referrer-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

User Credential Lists

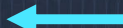


Automated Testing

Valid User Details



Account Takeover



Web



SQL



Credential stuffing demo

Account Protection

[Help](#)

Credential Stuffing Protection

Username Parameter

Name of the username parameter

Password Parameter

Name of the password parameter

Brute Force Prevention

Enable Bruteforce Prevention ☒ Yes ☐ No

Set to Yes to enable bruteforce prevention for this URL policy.

▼ [Advanced Configuration](#)



What is the URL we are going to protect?

BadStore.net - Register/Login

Not secure | demo.treacy.co.uk/cgi-bin/badstore.cgi?action=loginregister

BadStore.net

Welcome (Unregistered User) - Cart contains 0 items at \$0.00 [View Cart](#)

Search

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contract](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Login to Your Account or Register for a New Account

Login to Your Account

Email Address:

Password:

Register for a New Account

Full Name:

Email Address:

Password:

What's Your Favorite Color?: Green ▼

(The Password Hint is used as a security measure to help recover a forgotten password. You will need both your email address and this hint to access your account if you forget your current password.)

BadStore v1.2.3s - Copyright © 2004-2005

Bot Mitigation Policy: Configure URL Policy

Configure URL Policy

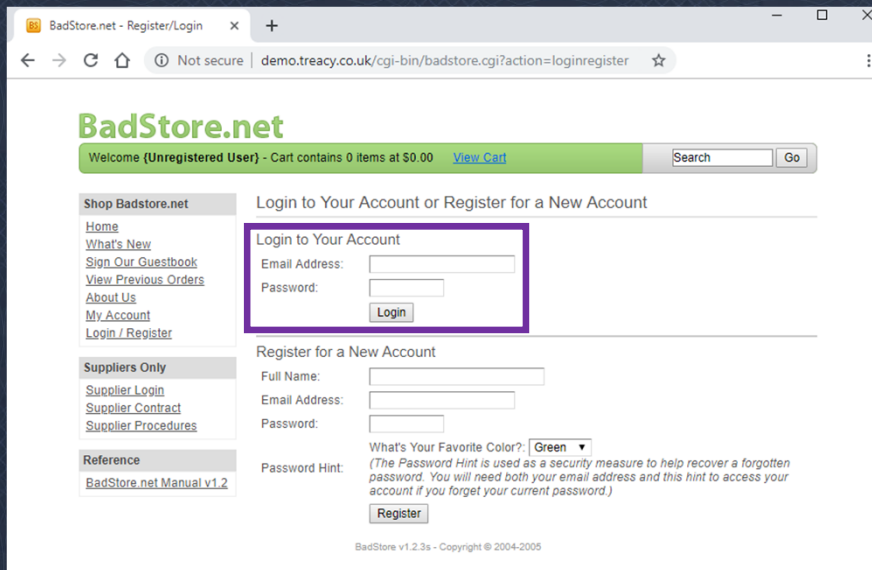
Help

URL Policy Name	<input type="text" value="Badstore_Login"/>
Status	<div>Specify a name for this URL policy.</div> <div><input checked="" type="radio"/> On <input type="radio"/> Off</div>
Mode	<div>Set to On to apply this URL Policy to the service.</div> <div><input type="radio"/> Passive <input checked="" type="radio"/> Active</div> <div>Active blocks any request when an anomaly or intrusion is observed. Passive logs all anomalies and intrusions found and allows the traffic to pass through the Barracuda Web Application Firewall.</div>
Host Match	<div><input type="text" value="*"/></div> <div>Specify the matching criterion for host field in the Request Header. This can be a specific host match or a wildcard host match with a single "*" anywhere in the URL. You can enter a partial domain with wildcard (for example: *.abc.com), but multiple asterisks cannot be used. Example: "*" *.abc.com www.abc.com</div>
URL Match	<div><input type="text" value="/cgi-bin/badstore.cgi"/></div> <div>Enter the matching criterion for the URL field in the Request Header. The URL should start with a "/" and can have only one "*" anywhere in the URL. A value of "*" means that the ACL applies for all URLs in that domain. Example: "/" /index.html /sub/index.html</div>
Extended Match	<div><input type="text" value="(Parameter action eq loginregister)"/></div> <div>Define an expression that consists of a combination of HTTP headers and/or query string parameters. This expression is used to match against special attributes in the HTTP headers or query string parameters in the requests.</div>
	<div><div>Header Expression: <input type="text" value="(Parameter action eq loginregister)"/></div><div><div>Element Type: <input type="text" value="Parameter"/></div><div>Element Name: <input type="text" value="\$ONAME_PARAM"/></div><div><input checked="" type="checkbox"/> Others' action</div></div><div><div>Operation: <input type="text" value="is equal to"/></div><div>Value: <input type="text" value="loginregister"/></div></div><div><div>Concatenate: <input checked="" type="radio"/> and <input type="radio"/> or <input type="button" value="Insert"/></div></div><div><div><input type="button" value="Apply"/></div><div><input type="button" value="Cancel"/></div></div></div>
Extended Match Sequence	<input type="text" value="1"/>
Comments	<div><div>Specify an order for matching the Extended Match rules to resolve conflicting URL ACLs that have the same Host Match, URL Match and Extended Match.</div><div><input type="text"/></div><div>Comments</div></div>

Bot Mitigation Policy: Configure URL Policy

Configure URL Policy		Help
URL Policy Name	<input type="text" value="Badstore_Login"/>	
	<small>Specify a name for this URL policy.</small>	
Status	<input checked="" type="radio"/> On <input type="radio"/> Off	
	<small>Set to On to apply this URL Policy to the service.</small>	
Mode	<input type="radio"/> Passive <input checked="" type="radio"/> Active	
	<small>Active blocks any request when an anomaly or intrusion is observed. Passive logs all anomalies and intrusions found and allows the traffic to pass through the Barracuda Web Application Firewall.</small>	
Host Match	<input type="text" value="*"/>	
	<small>Specify the matching criterion for host field in the Request Header. This can be a specific host match or a wildcard host match with a single "*" anywhere in the URL. You can enter a partial domain with wildcard (for example: "abc.com"), but multiple asterisks cannot be used. Example: " "abc.com www.abc.com</small>	
URL Match	<input type="text" value="/cgi-bin/badstore.cgi"/>	
	<small>Enter the matching criterion for the URL field in the Request Header. The URL should start with a "/" and can have only one "*" anywhere in the URL. A value of "/" means that the ACL applies for all URLs in that domain. Example: "/" /index.html /public/index.html</small>	
Extended Match	<input type="text" value="(Parameter action eq loginreq)"/>	
	<small>Define an expression that consists of a combination of HTTP headers and/or query string parameters. This expression is used to match against special attributes in the HTTP headers or query string parameters in the requests.</small>	
Extended Match Sequence	<input type="text" value="1"/>	
	<small>Specify an order for matching the Extended Match rules to resolve conflicting URL ACLs that have the same Host Match, URL Match and Extended Match.</small>	
Comments	<input type="text"/>	
	<small>Comments</small>	

What are the login parameters?



BadStore.net - Register/Login

Not secure | demo.treacy.co.uk/cgi-bin/badstore.cgi?action=loginregister

BadStore.net

Welcome (Unregistered User) - Cart contains 0 items at \$0.00 [View Cart](#)

Search

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contract](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Login to Your Account or Register for a New Account

Login to Your Account

Email Address:

Password:

Register for a New Account

Full Name:

Email Address:

Password:

What's Your Favorite Color?:

Password Hint:

(The Password Hint is used as a security measure to help recover a forgotten password. You will need both your email address and this hint to access your account if you forget your current password.)

Bot Mitigation Policy: Account Protection

Account Protection		Help
Credential Stuffing Protection		
Username Parameter	<input type="text"/>	
	<i>Name of the username parameter</i>	
Password Parameter	<input type="text"/>	
	<i>Name of the password parameter</i>	
Brute Force Prevention		
Enable Bruteforce Prevention	<input checked="" type="radio"/> Yes <input type="radio"/> No	
	<i>Set to Yes to enable bruteforce prevention for this URL policy.</i>	
▼ Advanced Configuration		

What is the Username Parameter name?

The screenshot displays the BadStore.net website interface. At the top, a green banner reads "Welcome Scott Treacy - Cart contains 0 Items at \$0.00" with a "View Cart" link and a search bar. The main content area is divided into three columns: a left sidebar with navigation links (Home, What's New, Sign Our Guestbook, View Previous Orders, About Us, My Account, Login / Register), a middle section for "Suppliers Only" (Supplier Login, Supplier Contact, Supplier Procedures), and a right section for "Reference" (BadStore.net Manual v1.2). The right section also contains two forms: "Login to Your Account or Register for a New Account" and "Register for a New Account". The login form has fields for "Email Address:" and "Password:" with a "Login" button. The registration form has fields for "Full Name:", "Email Address:", "Password:", and "What's Your Favorite Color?" (a dropdown menu set to "Green"). Below the registration form is a "Register" button. The bottom of the page shows the browser's developer tools with the "Elements" tab selected. The HTML structure is visible, showing a table with two columns: "Email Address:" and "Password:". The "Email Address:" input field is highlighted with a purple box, and its attributes are shown as `<input type="text" name="email" size="20" maxlength="40" >`. The "Password:" input field is shown as `<input type="password" name="passwd" size="8" maxlength="8" >`.

BadStore.net

Welcome Scott Treacy - Cart contains 0 Items at \$0.00 [View Cart](#)

Shop Badstore.net

- [Home](#)
- [What's New](#)
- [Sign Our Guestbook](#)
- [View Previous Orders](#)
- [About Us](#)
- [My Account](#)
- [Login / Register](#)

Suppliers Only

- [Supplier Login](#)
- [Supplier Contact](#)
- [Supplier Procedures](#)

Reference

- [BadStore.net Manual v1.2](#)

Login to Your Account or Register for a New Account

Login to Your Account

Email Address:

Password:

Register for a New Account

Full Name:

Email Address:

Password:

What's Your Favorite Color?: Green ▼

Password Hint: (The Password Hint is used as a security measure to help recover a forgotten password. You will need both your email address and this hint to access your account if you forget your current password.)

Elements Console Sources Network Performance Memory Application Security Audits

```
<div id="hd"></div>
<div id="bd">
  <div id="side"></div>
  <div id="main">
    <h2>Login to Your Account or Register for a New Account</h2>
    <h3>Login to Your Account</h3>
    <form method="post" action="/cgi-bin/badstore.cgi?action=login">
      <table cellpadding="0" cellspacing="0">
        <tbody>
          <tr>
            <td width="100">Email Address:</td>
            <td>
              <input type="text" name="email" size="20" maxlength="40" >
            </td>
          </tr>
          <tr>
            <td>Password:</td>
            <td>
              <input type="password" name="passwd" size="8" maxlength="8" >
            </td>
          </tr>
        </tbody>
      </table>
    </form>
  </div>
</div>
```


What is the Password Parameter name?

The screenshot displays the BadStore.net website interface. At the top, a green banner reads "Welcome Scott Treacy - Cart contains 0 Items at \$0.00" with a "View Cart" link. Below this is a navigation menu with links like "Home", "What's New", "Sign Our Guestbook", "View Previous Orders", "About Us", "My Account", and "Login / Register". The main content area is titled "Login to Your Account or Register for a New Account". It contains two sections: "Login to Your Account" with fields for "Email Address:" and "Password:" and a "Login" button; and "Register for a New Account" with fields for "Full Name:", "Email Address:", "Password:", and a "What's Your Favorite Color?" dropdown menu, followed by a "Register" button. A password hint is also provided.

The browser's developer tools are open at the bottom, showing the "Elements" panel. The HTML structure is expanded to the login form, and the password input field is highlighted. The code for the password field is:

```
<input type="password" name="password" size="8" maxlength="8" == $0 />
```

The attribute `name="password"` is highlighted with a red box, indicating the parameter name used for the password.

Bot Mitigation Policy: Account Protection

Account Protection		Help
Credential Stuffing Protection		
Username Parameter	<input type="text" value="email"/>	<small>Name of the username parameter</small>
Password Parameter	<input type="text" value="passwd"/>	<small>Name of the password parameter</small>
Brute Force Prevention		
Enable Bruteforce Prevention	<input checked="" type="radio"/> Yes <input type="radio"/> No	
<small>Set to Yes to enable bruteforce prevention for this URL policy.</small>		
▼ Advanced Configuration		

Testing some compromised user credentials

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#)

Shop Badstore.net
[Home](#)
[What's New](#)
[Sign Our Guestbook](#)
[View Previous Orders](#)
[About Us](#)
[My Account](#)
[Login / Register](#)

Suppliers Only
[Supplier Login](#)
[Supplier Contract](#)
[Supplier Procedures](#)

Reference
[BadStore.net Manual v1.2](#)

Login to Your Account or Register for a New Account

Login to Your Account

Email Address:

Password:

Register for a New Account

Full Name:

Email Address:

Password:

What's Your Favorite Color?:

Password Hint: (The Password Hint is used as a security measure to help recover a forgotten password. You will need both your email address and this hint to access your account if you forget your current password.)

BadStore v1.2.3s - Copyright © 2004-2005

WAF blocks with...

The request from 192.168.0.85 at 2019-05-15 11:54:22 GMT for the URL /cgi-bin/badstore.cgi cannot be served due to attack
CREDENTIAL_STUFFING_DETECTED Log ID is 16abb57e8a8-bf8a123b.

WAF logs...

Web Firewall Log Details[Help](#)

ALERT

2019-05-15 12:54:33
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

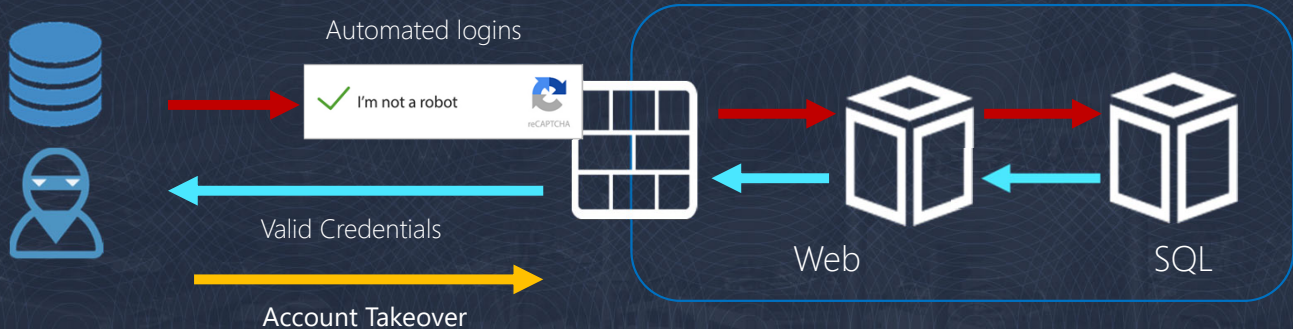
Attack	Credential Stuffing Detected
Attack Category	Bot Mitigation
Detail	Policy="service_192_168_0_170:BadStore_Login" User=julio.tan@gmail.com"

Credential cracking (With CAPTCHA defeat)

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

Additional automation required to defeat CAPTCHA

User Account Lists



reCAPTCHA demo

Captcha Settings

Help

Captcha Method

☐ CAPTCHA ☒ reCAPTCHA

Domains

Select Domains

Site key

Site Secret

Add

Search:

Domains	Actions
No data available in table	

Showing 0 to 0 of 0 entries

Previous

Next



Google reCAPTCHA settings: Create Domain

Label ⓘ

demo.treacy.co.uk

17/50

reCAPTCHA type ⓘ

☐ reCAPTCHA v3 Verify requests with a score

☒ reCAPTCHA v2 Verify requests with a challenge

☒ "I'm not a robot" textbox Validate requests with the "I'm not a robot" textbox

☐ Invisible reCAPTCHA badge Validate requests in the background

☐ reCAPTCHA Android Validate requests in your android app

Domains ⓘ


+ demo.treacy.co.uk

Google reCAPTCHA settings: Keys

Google reCAPTCHA


Adding reCAPTCHA to your site
'dem.treacy.co.uk' has been registered.

Use this site key in the HTML code your site serves to users. [See client side integration](#)

 COPY SITE KEY

6LcXn6MUAAAAAF4WkSL6KsYtBYMCYTxe9NC9vkIV

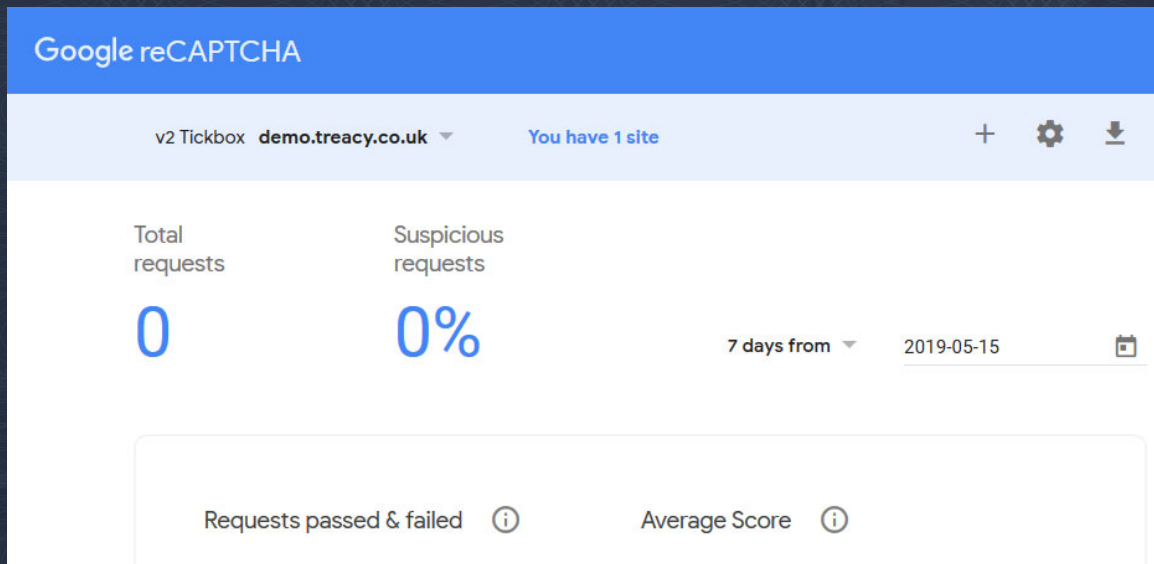
Use this secret key for communication between your site and reCAPTCHA. [See server side integration](#)

 COPY SECRET KEY

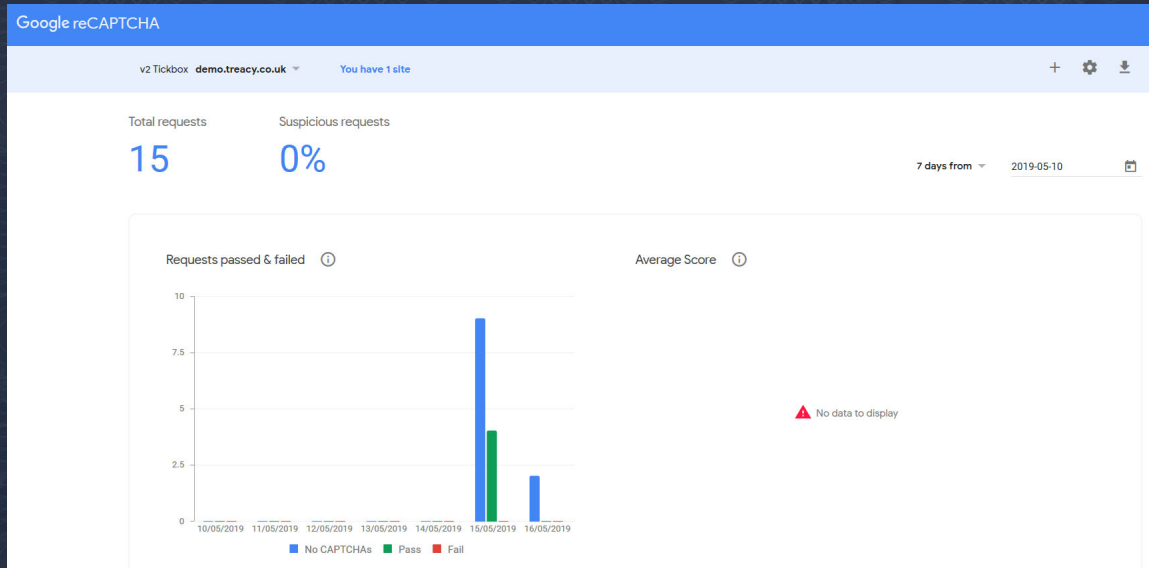
6LcXn6MUAAAAAC35jpt2BMRV3KEfziUwfNYZprXj

[GO TO SETTINGS](#) [GO TO ANALYTICS](#)

Google reCAPTCHA settings: Domain Admin



Google reCAPTCHA settings: Domain Admin



Barracuda WAF reCAPTCHA Service Settings

Captcha Settings

Help

Captcha Method

☐ CAPTCHA ☒ reCAPTCHA

Domains

Add New Domain ▼

Domain

demo.treacy.co.uk

Site key

.....

Site Secret

.....

Add

Search:

Domains	Actions
No data available in table	

Showing 0 to 0 of 0 entries

Previous

Next

Barracuda WAF reCAPTCHA Service Settings

Captcha Settings

Help

Captcha Method

☐ CAPTCHA ☒ reCAPTCHA

Domains

Add New Domain ▼

Domain

The Domain which is to be challenged with selected captcha method

Site key

Add the domain to be challenged with reCAPTCHA

Site Secret

Add the reCAPTCHA Site key for the selected domain

Add the reCAPTCHA secret for the selected domain

Add

Search:

Domains	Actions
demo.treacy.co.uk	Delete

Showing 1 to 1 of 1 entries

Previous

1

Next

Barracuda WAF reCAPTCHA Service Settings

Captcha Settings

Help

Captcha Method

☐ CAPTCHA ☒ reCAPTCHA

Domains

Captcha type to be presented to the user

demo.treacy.co.uk

Select Domains

Add New Domain

demo.treacy.co.uk

Add

Site key

Site Secret

selected domain

selected domain

Search:

Domains	Actions
demo.treacy.co.uk	Delete

Showing 1 to 1 of 1 entries

Previous

1

Next

Barracuda WAF DDoS Policy CAPTCHA settings

Add DDoS Policy

Help

DDoS Policy Name

BadStore_Login

Host Match

*

Specify a name for this DDoS Policy.

URL Match

/cgi-bin/badstore.cgi

Specify the matching criterion for host field in the Request Header. This can be a specific host match or a wildcard host match with a single "*" anywhere in the URL. You can enter a partial domain with wildcard (for example: *.abc.com), but multiple asterisks cannot be used.
Example: *
*.abc.com
www.abc.com

Extended Match

*

Enter the matching criterion for the URL field in the Request Header. The URL should start with a "/" and can have only one "*" anywhere in the URL. A value of /* means that the ACL applies for all URLs in that domain.
Example: /*
/index.html
/public/index.html

Header

(Parameter action eq loginregister)

Expression:

Element Type:

Parameter

Element Name:

\$NONAME_PARAM

☒ Others

action

Operation:

is equal to

Value:

loginregister

Concatenate:

☐ and ☐ or

Insert

Apply

Cancel

Barracuda WAF DDoS Policy CAPTCHA settings

Add DDoS Policy		Help
DDoS Policy Name	<input type="text" value="BadStore_Login"/> <small>Specify a name for this DDoS Policy.</small>	
Host Match	<input type="text" value="*"/> <small>Specify the matching criterion for host field in the Request Header. This can be a specific host match or a wildcard host match with a single "*" anywhere in the URL. You can enter a partial domain with wildcard (for example: *.abc.com), but multiple asterisks cannot be used. Example: * *.abc.com www.abc.com</small>	
URL Match	<input type="text" value="/cgi-bin/badstore.cgi"/> <small>Enter the matching criterion for the URL field in the Request Header. The URL should start with a "/" and can have only one "*" anywhere in the URL. A value of /* means that the ACL applies for all URLs in that domain. Example: /* index.html public/index.html</small>	
Extended Match	<input type="text" value="(Parameter action eq loginreq)"/> <small>An expression made up of various HTTP header components, to match requests with special attributes in the HTTP Headers or query string parameters. The token is case sensitive.</small>	
Extended Match Sequence	<input type="text" value="1"/> <small>The order in which to evaluate this rule's Extended Match expression when a request matches multiple rules with the same URL Match and Host match.</small>	
Evaluate Clients	<input checked="" type="radio"/> On <input type="radio"/> Off <small>Specifies whether or not track and detect and mark suspected bots or non browser based user agents.</small>	
Enforce CAPTCHA	<div><div>Do not Enforce</div><div>Enforce on suspicious clients only</div><div>All clients</div></div> <small>If set to 'Yes', the JavaScript gets executed only when the "Mousemove" event is detected in the client's browser.</small>	
Max CAPTCHA Attempts	<input type="text" value="5"/> <small>Specifies the number of attempts a client can make for solving the CAPTCHA challenge.</small>	
Max Unanswered CAPTCHA	<input type="text" value="100"/> <small>Specifies the limit for the number of unanswered CAPTCHAs challenged to a specific Client IP.</small>	
Expiry time	<input type="text" value="300"/> <small>Specifies the number of seconds the client can be idle once validated. The client will be challenged back when a request comes in after this period.</small>	
Comments	<input type="text"/>	

Barracuda WAF DDoS Policy CAPTCHA settings

Add DDoS Policy		Help
DDoS Policy Name	<input type="text" value="BadStore_Login"/> <small>Specify a name for this DDoS Policy.</small>	
Host Match	<input type="text" value="*"/> <small>Specify the matching criterion for host field in the Request Header. This can be a specific host match or a wildcard host match with a single "*" anywhere in the URL. You can enter a partial domain with wildcard (for example: *.abc.com), but multiple asterisks cannot be used. Example: * *.abc.com www.abc.com</small>	
URL Match	<input type="text" value="/cgi-bin/badstore.cgi"/> <small>Enter the matching criterion for the URL field in the Request Header. The URL should start with a "/" and can have only one "*" anywhere in the URL. A value of /* means that the ACL applies for all URLs in that domain. Example: /* index.html public/index.html</small>	
Extended Match	<input type="text" value="(Parameter action eq login)"/> <small>An expression made up of various HTTP header components, to match requests with special attributes in the HTTP Headers or query string parameters. The token is case sensitive.</small>	
Extended Match Sequence	<input type="text" value="1"/> <small>The order in which to evaluate this rule's Extended Match expression when a request matches multiple rules with the same URL Match and Host match.</small>	
Evaluate Clients	<input checked="" type="radio"/> On <input type="radio"/> Off <small>Specifies whether or not track and detect and mark suspected bots or non browser based user agents.</small>	
Enforce CAPTCHA	<input type="text" value="All clients"/> <small>Specifies whether the CAPTCHA needs to be enforced on all clients, or only for suspected clients which are found suspicious by the fingerprinting module.</small>	
Detect Mouse Event	<input checked="" type="radio"/> On <input type="radio"/> Off <small>If set to Yes, the JavaScript gets executed only when the "Mousemove" event is detected in the client's browser.</small>	
Max CAPTCHA Attempts	<input type="text" value="5"/> <small>Specifies the number of attempts a client can make for solving the CAPTCHA challenge.</small>	
Max Unanswered CAPTCHA	<input type="text" value="100"/> <small>Specifies the limit for the number of unanswered CAPTCHAs challenged to a specific Client IP.</small>	
Expiry time	<input type="text" value="300"/> <small>Specifies the number of seconds the client can be idle once validated. The client will be challenged back when a request comes in after this period.</small>	
Comments	<input type="text"/>	

The BadStore... Lets Login!

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#)

Shop Badstore.net

[Home](#)
[What's New](#)
[Sign Our Guestbook](#)
[View Previous Orders](#)
[About Us](#)
[My Account](#)
[Login / Register](#)

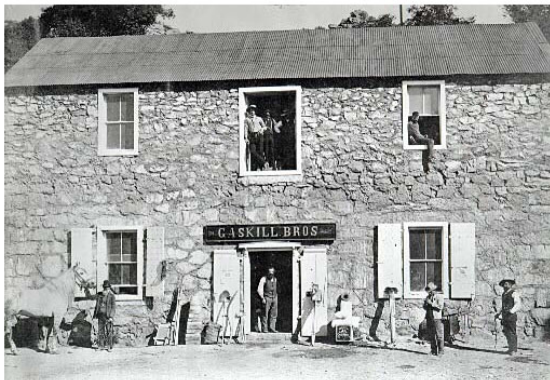
Suppliers Only

[Supplier Login](#)
[Supplier Contract](#)
[Supplier Procedures](#)

Reference

[BadStore.net Manual v1.2](#)


Welcome to BadStore.net!




BadStore v1.2.3s - Copyright © 2004-2005

Barracuda WAF inserts the reCAPTCHA...

User validation required to continue..

 I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

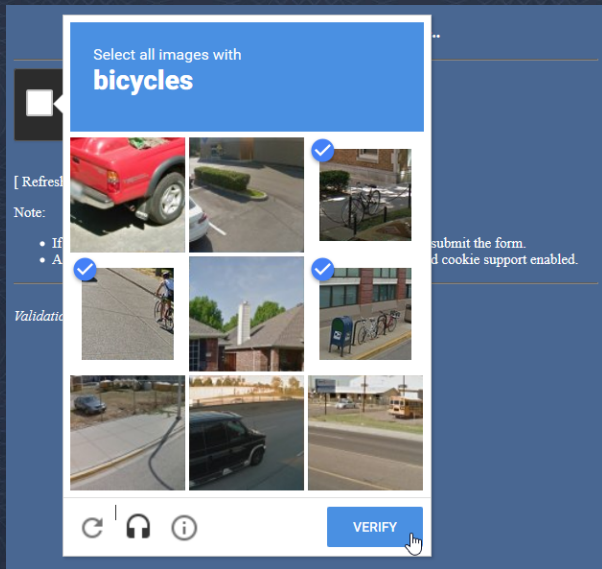
[Refresh the page to generate a new image.]

Note:

- If you get here while trying to submit a form, you may have to re-submit the form.
- Access to this domain may need the browser to have javascript and cookie support enabled.

Validation needed due to : **Policy constraints**

reCAPTCHA verify (if Google are suspicious)...



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

User validation required to continue..

Please type the text you see in the image into the text box and submit

[Refresh the page to generate a new image.]

Note:

- If you get here while trying to submit a form, you may have to re-submit the form.
- Access to this domain may need the browser to have javascript and cookie support enabled.

Validation needed due to : **Policy constraints**
Number of attempts left : **5**

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

BadStore.net

Welcome {Unregistered User} Cart contains 0 items at \$0.00 [View Cart](#)

Shop Badstore.net
[Home](#)
[What's New](#)
[Sign Our Guestbook](#)
[View Previous Orders](#)
[About Us](#)
[My Account](#)
[Login / Register](#)

Suppliers Only
[Supplier Login](#)
[Supplier Contract](#)
[Supplier Procedures](#)

Reference
[BadStore.net Manual v1.2](#)

Login to Your Account or Register for a New Account

Login to Your Account
Email Address:
Password:

Register for a New Account
Full Name:
Email Address:
Password:
What's Your Favorite Color?:
Password Hint: (The Password Hint is used as a security measure to help recover a forgotten password. You will need both your email address and this hint to access your account if you forget your current password.)

BadStore v1.2.3s - Copyright © 2004-2005

...and now Logged in

BadStore.net

Welcome **Scott Treacy** - Cart contains 0 items at \$0.00

[View Cart](#)

Search

Go

Shop Badstore.net

[Home](#)
[What's New](#)
[Sign Our Guestbook](#)
[View Previous Orders](#)
[About Us](#)
[My Account](#)
[Login / Register](#)

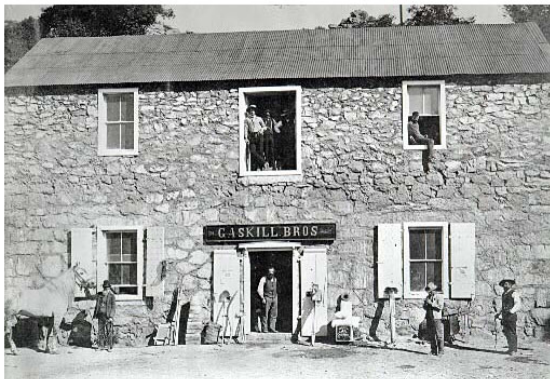
Suppliers Only

[Supplier Login](#)
[Supplier Contract](#)
[Supplier Procedures](#)

Reference

[BadStore.net Manual v1.2](#)

Welcome to BadStore.net!



BadStore v1.2.3s - Copyright © 2004-2005

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