OWASP
Open Web Application Security Project

CRS
THE 1ST LINE OF DEFENSE

Christian Folini / @ChrFolini

Introducing the OWASP ModSecurity Core Rule Set 3.0

Seat Belts

Defense in Depth • 1st Line of Defense

The Plan for Today

- What is a WAF / what is ModSecurity?
- What is the Core Rule Set 3.0 (CRS3)
- Installation (Demo)
- Burp Research Results

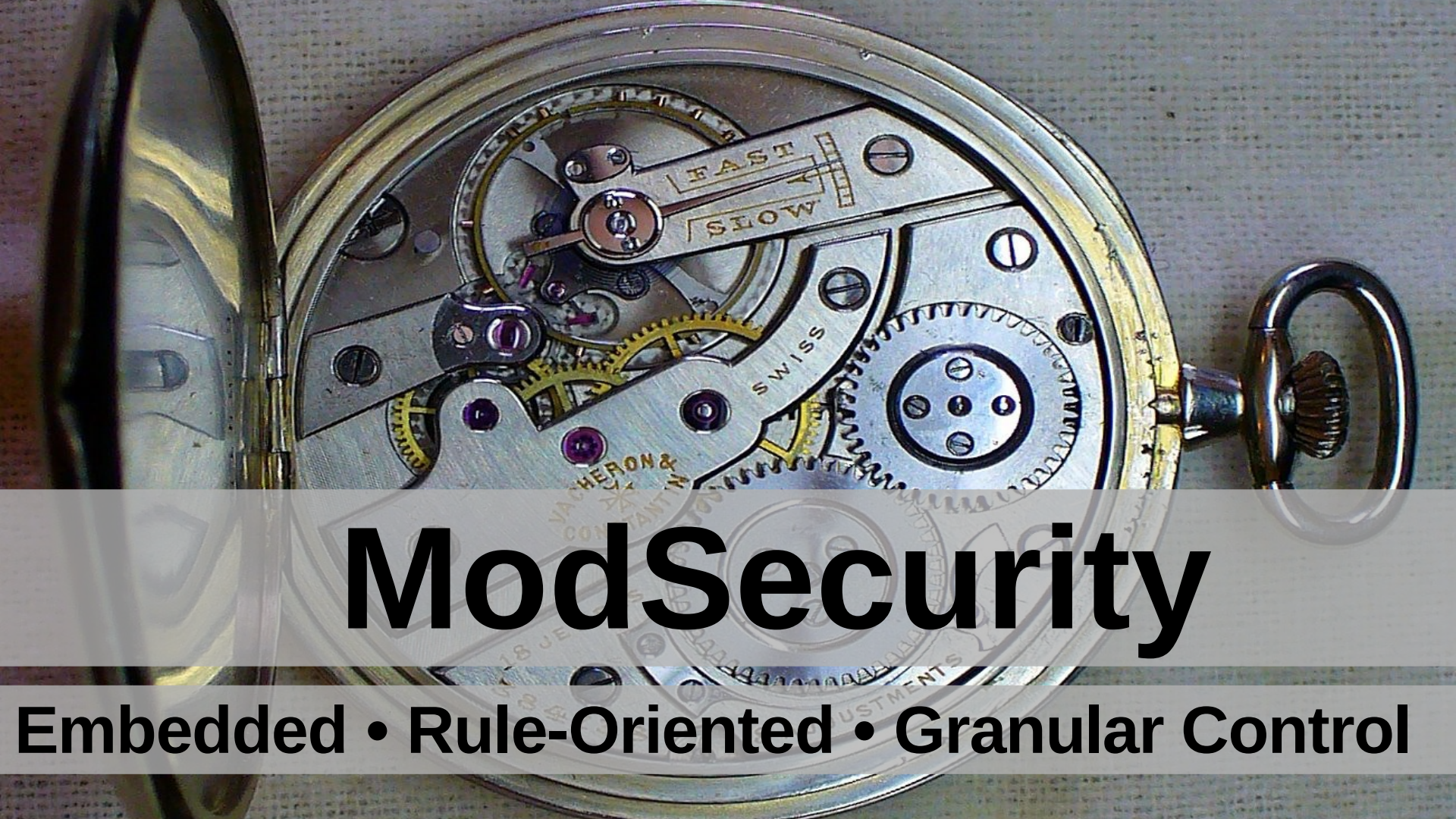
- Important Groups of Rules
- Anomaly Scoring / Thresholds
- Paranoia Levels / Stricter Siblings

- Sampling Mode
- Handling of False Positives
- Predefined Rule Exclusions

CRS

THE 1ST LINE OF DEFENSE


WAF SETUPS
Naïve • Overwhelmed • Functional



ModSecurity

Embedded • Rule-Oriented • Granular Control


INCLUDES DR. FOLINI'S PARANOIA MODE
OWASP ModSecurity Core Rule Set
v3.0
BASED UPON A TRUE STORY!
CRS3
OWASP ModSecurity Core Rule Set v3.0
DIRECTED BY
CHAIM SANDERS
STARRING
WALTER HOP AS REGEX WIZARD, CHAIM SANDERS
ORIGINAL IDEA BY OFER SHEZAF AND RYAN BARNETT ALSO STARRING CHRISTIAN FOLINI, FRANZISKA BÜHLER, @EMPHAZER, RYAN BARNETT, FELIPE 'ZIMMERLE' MANUEL LEOS, VLADIMIR IVANOV, CHRISTIAN PERON, @YGREK, @TOBY78, @JAMUSE, MATT KOCH, ACHIM HOFFMANN, MAZIN AHMED, NOËL ZINDEL
Trustwave Smart security on demand
COMING SOON TO A SERVER NEAR YOU!
OWASP Open Web Application Security Project

Installation

Clone the repository:

```
$> git clone
    https://github.com/SpiderLabs/owasp-modsecurity-crs
```

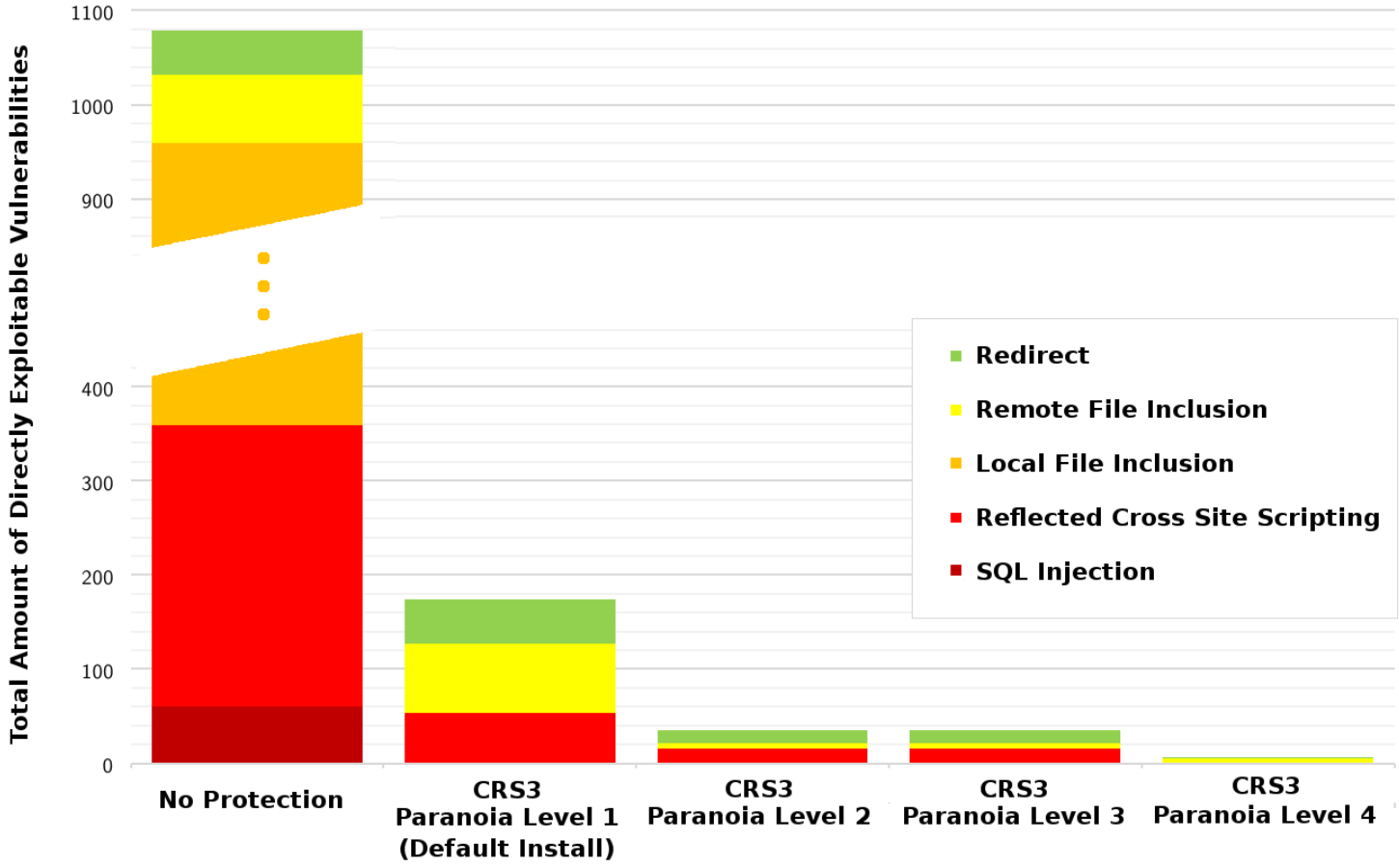
Copy the example config:

```
$> cp crs-setup.conf.example crs-setup.conf
```

Include in server config (depending on path):

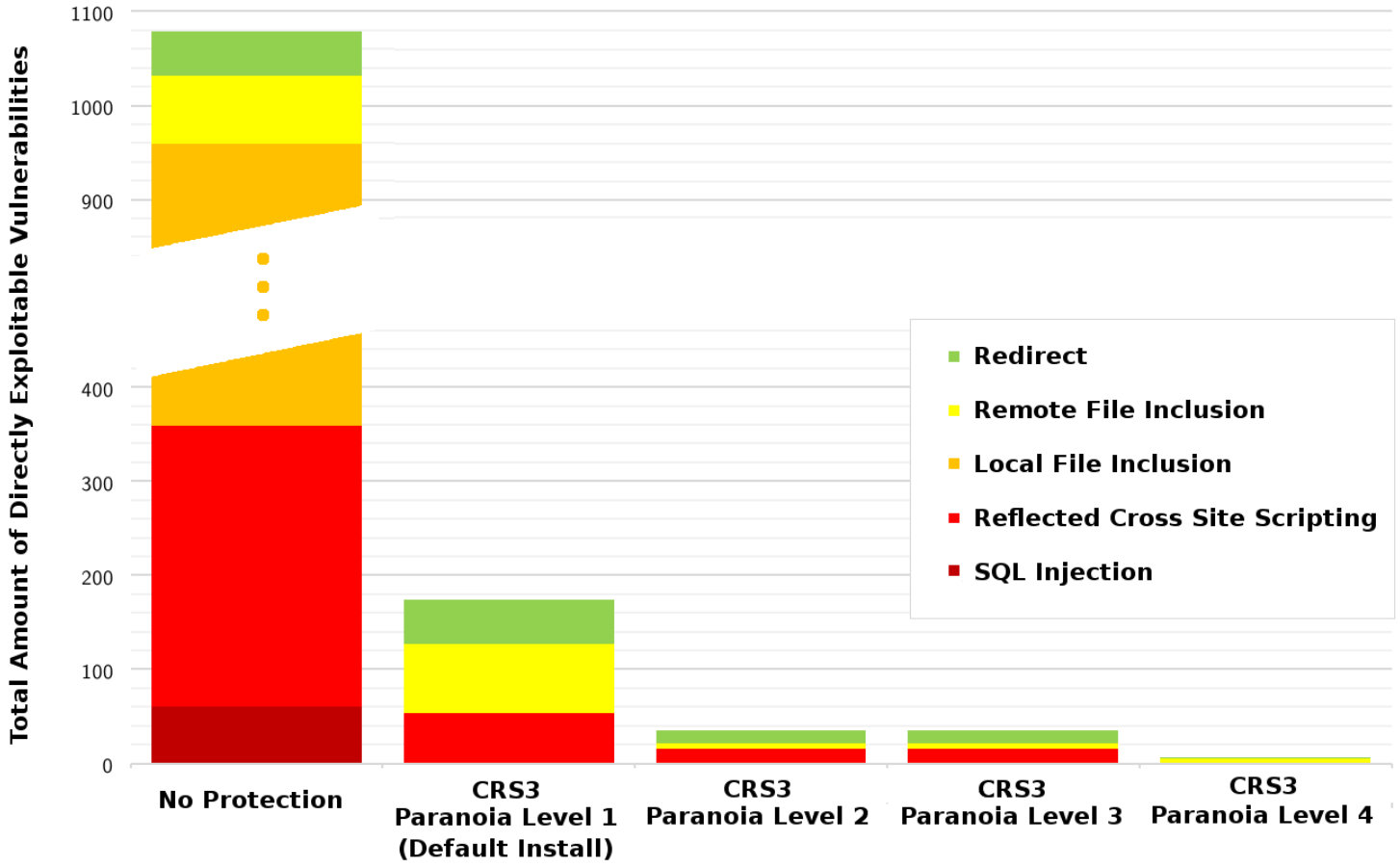
```
Include /etc/httpd/modsec.d/owasp-modsecurity-crs/crs-setup.conf

Include /etc/httpd/modsec.d/owasp-modsecurity-crs/rules/*.conf
```

Burp vs. OWASP ModSecurity Core Rule Set 3.0



Research based on 4.5M Burp requests.

Burp vs. OWASP ModSecurity Core Rule Set 3.0



CRS3
Default Install

Redir.:	0%
RFI:	0%
LFI:	**-100%**
XSS:	**-82%**
SQLi:	**-100%**

Research based on
4.5M Burp requests.

Important Groups of Rules

Rules Targetting the Request

REQUEST-910-IP-REPUTATION.conf
REQUEST-911-METHOD-ENFORCEMENT.conf
REQUEST-912-DOS-PROTECTION.conf
REQUEST-913-SCANNER-DETECTION.conf
REQUEST-920-PROTOCOL-ENFORCEMENT.conf
REQUEST-921-PROTOCOL-ATTACK.conf

REQUEST-930-APPLICATION-ATTACK-LFI.conf
REQUEST-931-APPLICATION-ATTACK-RFI.conf
REQUEST-932-APPLICATION-ATTACK-RCE.conf
REQUEST-933-APPLICATION-ATTACK-PHP.conf
REQUEST-941-APPLICATION-ATTACK-XSS.conf
REQUEST-942-APPLICATION-ATTACK-SQLI.conf
REQUEST-943-APPLICATION-ATTACK-SESS-FIX.conf

REQUEST-949-BLOCKING-EVALUATION.conf

CRS

THE 1ST LINE OF DEFENSE

Important Groups of Rules

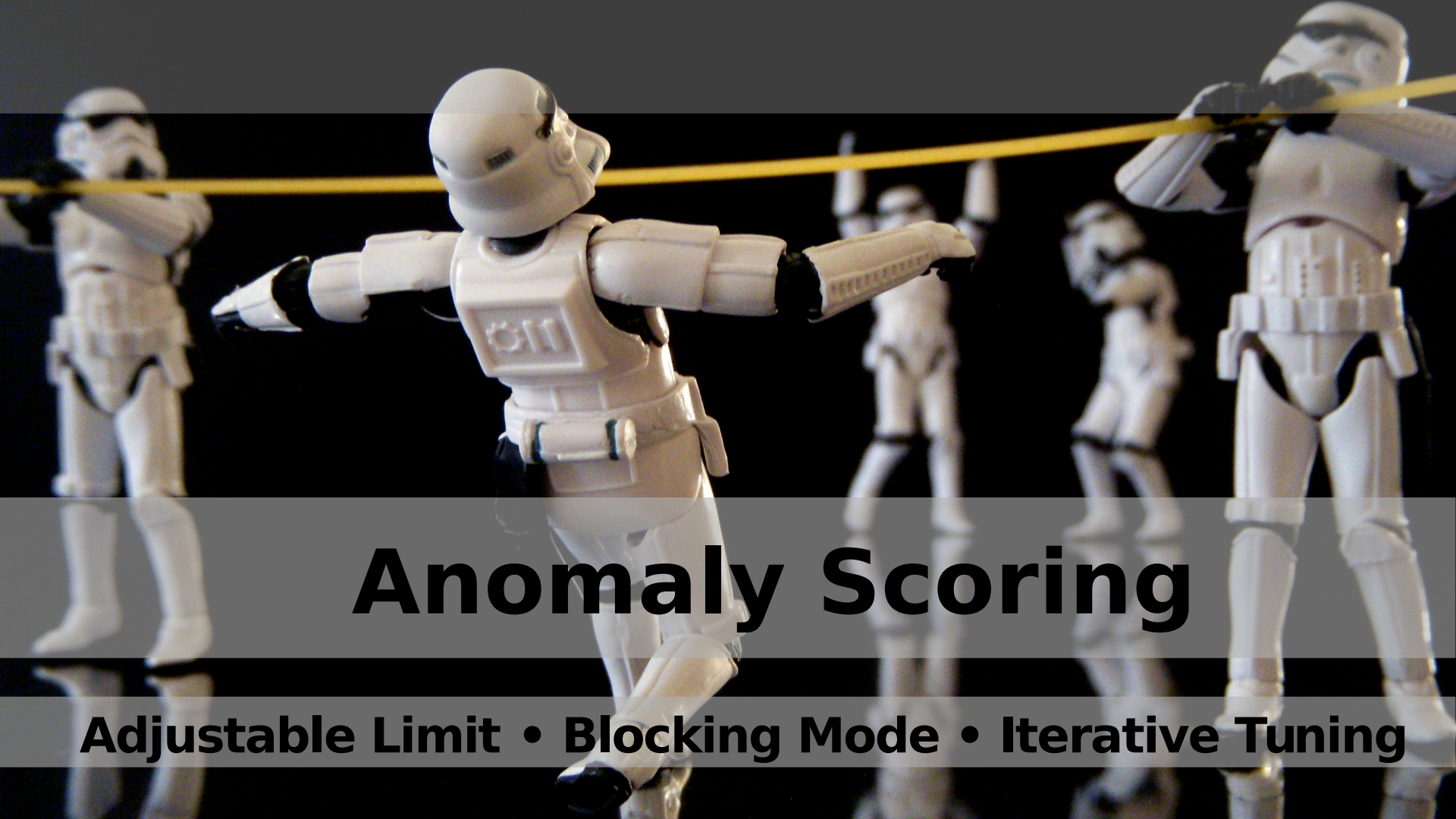
SLAC
BERLIN

Rules Targetting the Response

RESPONSE-950-DATA-LEAKAGES.conf
RESPONSE-951-DATA-LEAKAGES-SQL.conf
RESPONSE-952-DATA-LEAKAGES-JAVA.conf
RESPONSE-953-DATA-LEAKAGES-PHP.conf
RESPONSE-954-DATA-LEAKAGES-IIS.conf

RESPONSE-959-BLOCKING-EVALUATION.conf

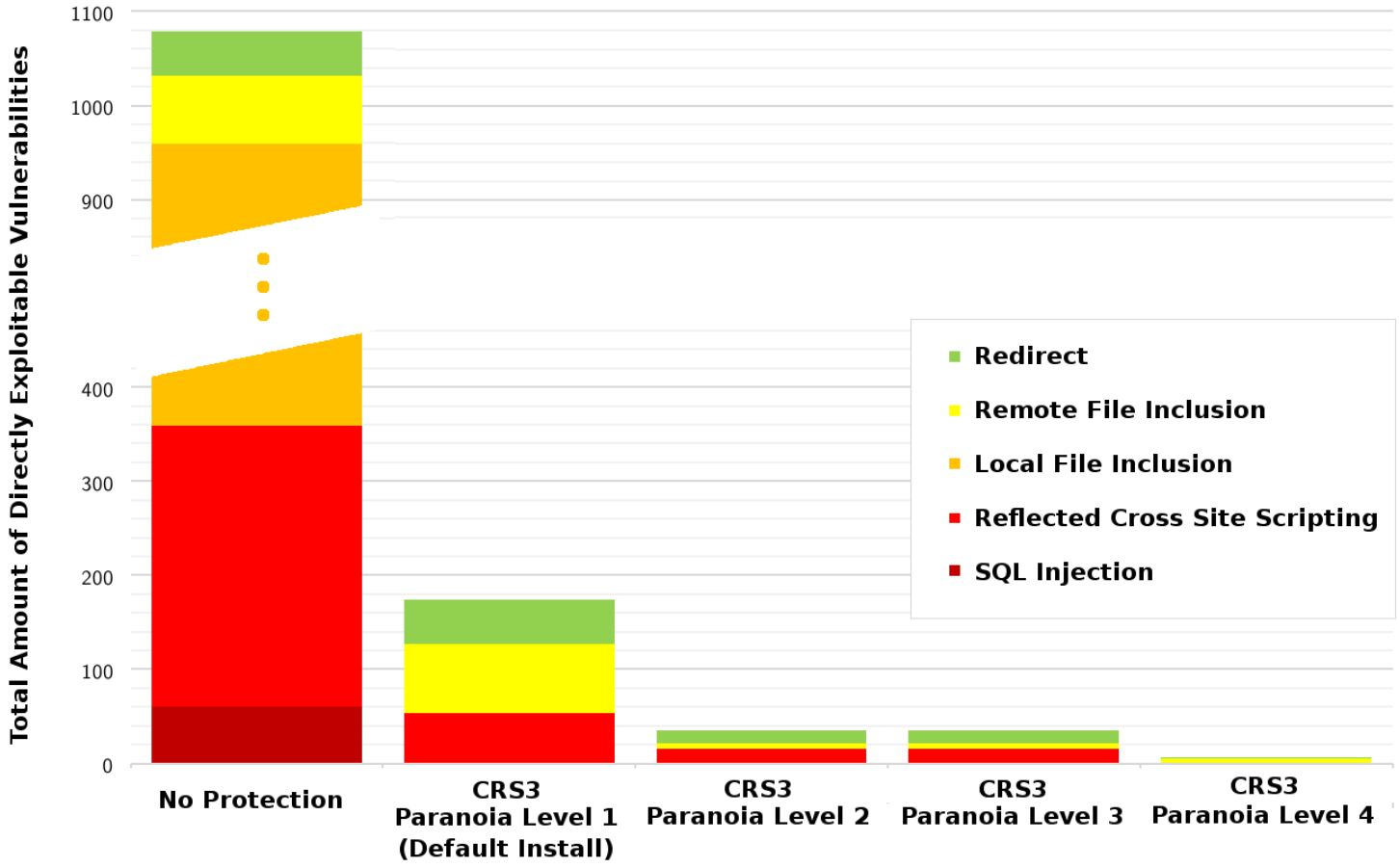
CRS
THE 1ST LINE OF DEFENSE



Anomaly Scoring

Adjustable Limit • Blocking Mode • Iterative Tuning

Burp vs. OWASP ModSecurity Core Rule Set 3.0



CRS3 Default Install

Redir.:	0%
RFI:	0%
LFI:	**-100%**
XSS:	**-82%**
SQLi:	**-100%**

Research based on 4.5M Burp requests.

Paranoia Levels

Paranoia Level 1: Minimal amount of False Positives
Basic security

Paranoia Level 2: More rules, fair amount of FPs
Elevated security level

Paranoia Level 3: Specialised rules, more FPs
Online banking level security

Paranoia Level 4: Insane rules, lots of FPs
Nuclear power plant level security

CRS
THE 1ST LINE OF DEFENSE

Paranoia Levels

Example: Protocol Enforcement Rules

Paranoia Level 1: 31 rules

Paranoia Level 2: 7 rules

Paranoia Level 3: 1 rule

Paranoia Level 4: 4 rules

CRS

THE 1ST LINE OF DEFENSE

Stricter Siblings

SLAC
BERLIN

Example: Byte Range Enforcement

Paranoia Level 1:
Rule 920270: Full ASCII range without null character

Paranoia Level 2:
Rule 920271: Full visible ASCII range, tab, newline

Paranoia Level 3:
Rule 920272: Visible lower ASCII range without %

Paranoia Level 4:
Rule 920273: A-Z a-z 0-9 = - _ . , : &

CRS
THE 1ST LINE OF DEFENSE

Sampling Mode

Limit CRS Impact During Proof of Concept

- Define sampling percentage n
- Only n% of requests are funnelled into CRS3
- 100%-n% of requests are unaffected by CRS3

CRS

THE 1ST LINE OF DEFENSE

False Positives

False Positives will haunt you from PL2

- **Fight FPs with Rule Exclusions**
- **Follow Tutorials at https://www.netnea.com**
- **Download Cheatsheet from Netnea**

Predefined Rule Exclusions

Enable Rule Exclusions for Specific Applications

CRS
THE 1ST LINE OF DEFENSE

Currently Supported:

- Wordpress (Default install)
- Drupal (Core)

In the Queue:

- DokuWiki
- OwnCloud / NextCloud

... contributions welcome!

Roundup CRS3

SLAC
BERLIN

- 1st Line of Defense against web attacks
- Generic set of blacklisting rules for WAFs
- Prevents 80% of web attacks with minimal FPs
- Gives you granular control on indiv. Parameters

More infos at https://coreruleset.org

CRS

THE 1ST LINE OF DEFENSE

Q&A CRS3

Christian Folini

SLAC
BERLIN

ModSecurity / CRS Tutorials: https://www.netnea.com

ModSecurity / CRS Course: Zurich, September 2018

Contact me at: christian.folini@netnea.com

@ChrFolini