

# How to run a successful internal bug bounty program

---

February 27<sup>th</sup>, 2019



# Persona

---

IT Security Engineer

 [PascalSec](#)



Pascal Schulz



"From dozens of monitoring tools to one intelligent platform.  
**Only Dynatrace.**"

**Mark Kaplan**, Director of IT at BARBRI

[Free trial](#)[▶ See the magic](#)

# **Reminder:**

# **What is a Bug Bounty Program?**

---

# Where did the idea come from?

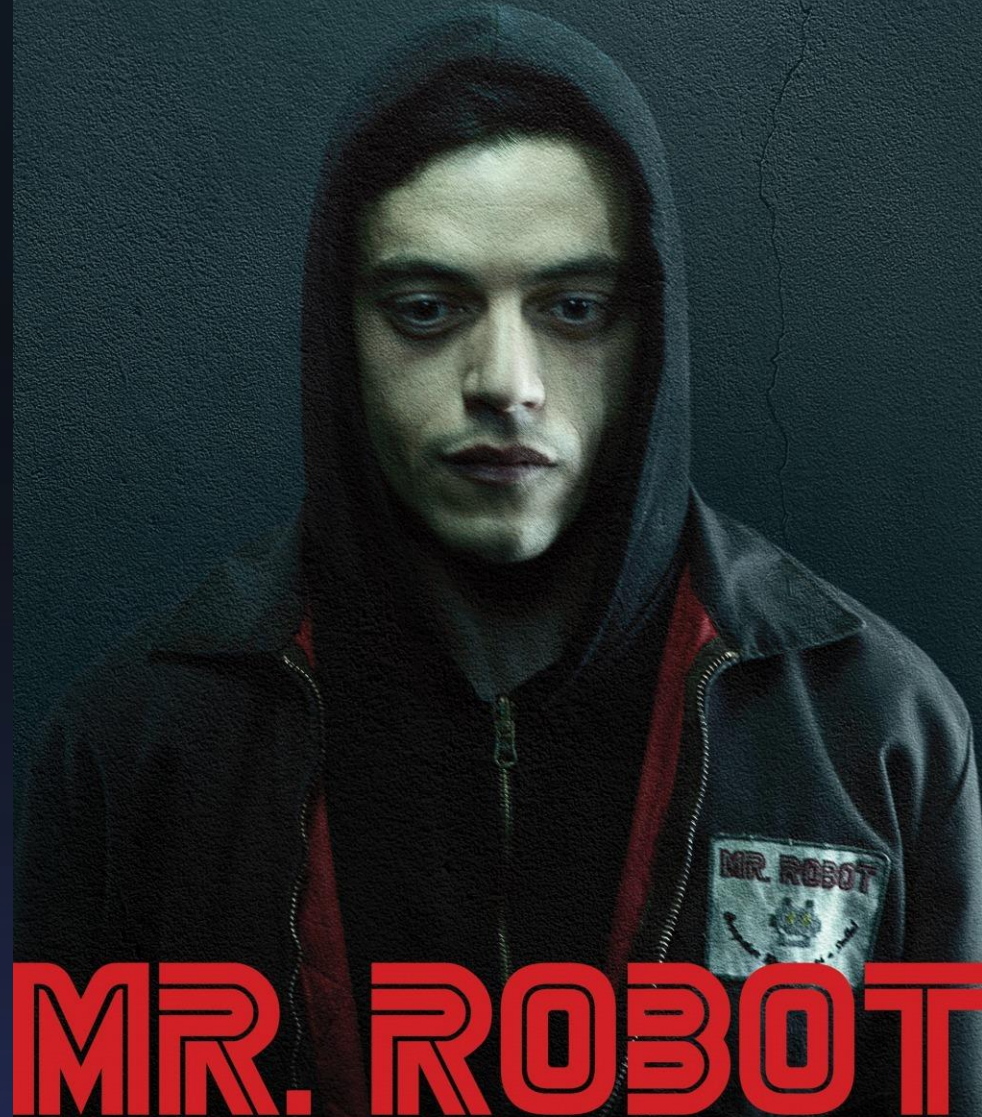
---

# Finding a theme

---



CONTROL IS AN ILLUSION



**MR. ROBOT**

season\_2.0 | 7.13 **usa**

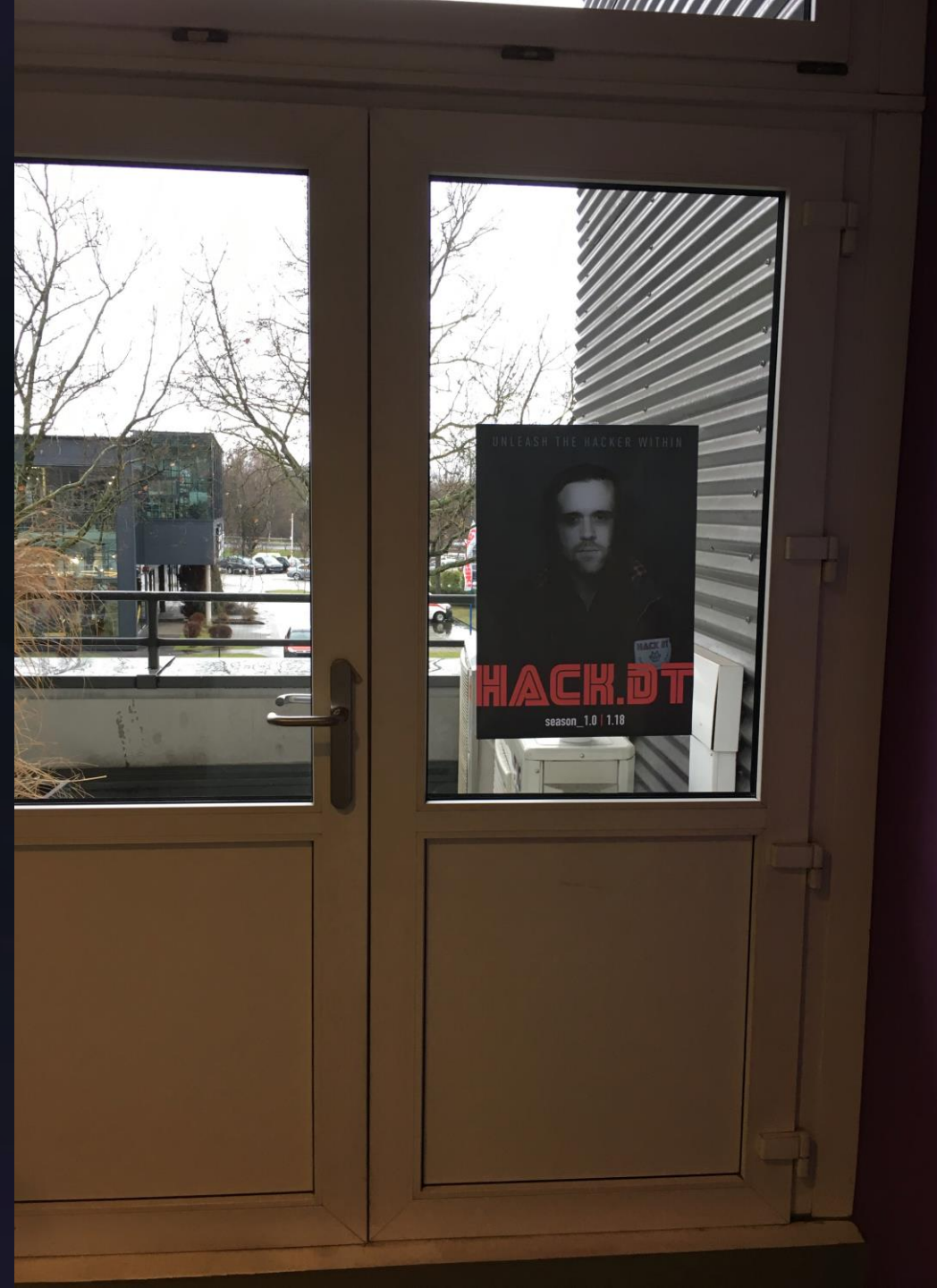
UNLEASH THE HACKER WITHIN



**HACK.DT**

season\_1.0 | 1.18 **LNZ**



















# Demo

---


# Setting up the program

---

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

- [Who can participate in the bug bounty program?](#)
- [Program Rules](#)
- [Scope and Eligible Vulnerabilities](#)
- [Rewards](#)
- [Program Exclusions](#)
- [Process](#)
- [Findings](#)

Key Information	
Runtime	January 18th - February 28th
Budget	Initially: \$ 10.000, upgraded to \$ 20.000 (\$ 7.240 left)
JIRA Project	<a href="https://[redacted]projects/HDT/">https://[redacted]projects/HDT/</a>
JIRA Label	<a href="#">BugBounty_Q12018</a>
Test Environment	SaaS: [redacted] Managed: [redacted]
Ticket to book time	 <a href="#">APM-118291</a> <a href="#">OPEN</a>
Primary Contact	<a href="#">@Schulz, Pascal</a>

[Who can participate in the bug bounty program?](#)



# Bug

Created t

- W
- P
- S
- R
- P
- P
- F

## Key In

Runtime	January 18th - February 28th
Budget	Initially: \$ 10.000, upgraded to \$ 20.000 (\$ 7.24
JIRA Project	<a href="https://projects/HDT/">https:// projects/HDT/</a>
JIRA Label	BugBounty_Q12018
Test Environment	SaaS: Managed:
Ticket to book time	<a href="#">APM-118291</a> OPEN
Primary Contact	@Schulz, Pascal




Who can participate in the bug bounty program?

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018


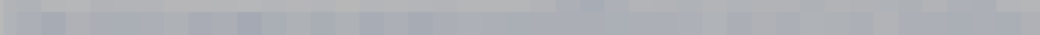

- Who can participate in the bug bounty program?
- Program Rules

Key Information	
Runtime	January 18th - February 28th
Budget	Initially: \$ 10.000, upgraded to \$ 20.000 (\$ 7.240 left)
JIRA Project	<a href="https://[redacted]/projects/HDT/">https://[redacted]/projects/HDT/</a>
JIRA Label	<a href="#">BugBounty_Q12018</a>
Test Environment	SaaS: [redacted] Managed: [redacted]
Ticket to book time	 <a href="#">APM-118291</a> <span>OPEN</span>
Primary Contact	<a href="#">@Schulz, Pascal</a>

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

- Who can participate in the bug bounty program?
- Program Rules
- Scope and Eligible Vulnerabilities
- Rewards
- Program Exclusions
- Process
- Findings

Test Environment	SaaS: 
	Managed: 
Ticket to book time	 APM-118291 <span>OPEN</span>
Primary Contact	<span>@Schulz, Pascal</span>

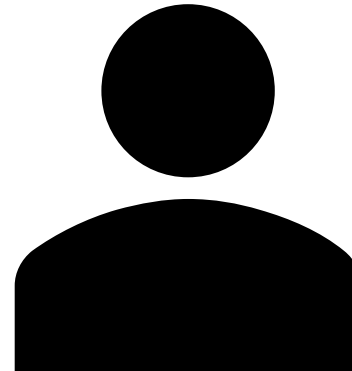



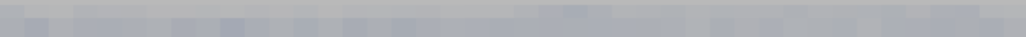

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

## ➔ Who can participate in the bug bounty program?

- Program Rules
- Scope and Eligible Vulnerabilities
- Rewards
- Program Exclusions
- Process
- Findings



Test Environment	SaaS: 
	Managed: 
Ticket to book time	 APM-118291 <span>OPEN</span>
Primary Contact	@Schulz, Pascal

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

- Who can participate in the bug bounty program?

## → Program Rules

- Scope and Eligible Vulnerabilities
- Rewards
- Program Exclusions
- Process

1. Time spent working on finding a bounty is never an excuse to delay your official tasks (the time to fix reported issues obviously is an official task).
2. Vulnerabilities in code you own are not eligible for a reward.
3. All tests need to be done within the current bug bounty's test environment (see key information above).
4. If you find a vulnerability and want to test if it affects production, please contact [@Schulz, Pascal](#) first.
5. Security vulnerabilities that are already documented in JIRA at the time of submission do not qualify for a reward.
6. Issues created from support cases are not eligible for a reward.
7. Do not try to trick the bug bounty program in any way in order to earn a reward.
8. Don't expose any security vulnerability findings to anybody else than internal colleagues (even after the finding has been fixed).
9. In case any sensitive information of a colleague is disclosed, please report the finding in private.

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

- Who can participate in the bug bounty program?

- Program Rules

- ➔ Scope and Eligible Vulnerabilities

- Rewards

- Program Exclusions

- Process

- Missing security headers including (content security policy) which do not lead directly to a vulnerability
- Clickjacking on static websites
- Vulnerabilities affecting users of outdated browsers or platforms
- Presence of autocomplete attribute on web forms
- HTTP 404 codes/pages or other HTTP non-200 codes/pages
- Disclosure of known public files or directories, (e.g. robots.txt)
- HTTP methods enabled other than GET/POST
- Weak password policies



# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

- Who can participate in the bug bounty program?
- Program Rules
- Scope and Eligible Vulnerabilities
- ➔ Rewards
- Program Exclusions
- Process

CVSS Severity Level	Score Range	Multiplication Factor	Possible Rewards*	CVSS ↔ JIRA Priority Mapping
Informational	0	0	0	Undefined
Low	0.1 - 3.9	25	\$ 2,5 - 97,5	Minor
Medium	4.0 - 6.9	50	\$ 200 - 345	Critical
High	7.0 - 8.9	75	\$ 525 - 667,5	Blocker
Critical	9.0 - 10.0	100	\$ 900 - 1000	Emergency

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

- Who can participate in the bug bounty program?
- Program Rules
- Scope and Eligible Vulnerabilities
- Rewards
- ➔ Program Exclusions
- Process

- Harmful activities against production environments
- (Spear-) Phishing Attacks
- Social-Engineering Attacks
- Attacking 3rd-Party Providers
- Do not change any data that does not belong to you
- Usage of automated tools in case it is not well understood what the tool is actually performing
- Do not perform any kind of physical attacks (unplugging computers, breaking doors, etc.)

# Bug Bounty Program

Created by Schulz, Pascal, last modified on Mar 30, 2018

- Who can participate in the bug bounty program?
- Program Rules
- Scope and Eligible Vulnerabilities
- Rewards
- Program Exclusions
- ➔ Process
- Finding

- Test the product, which is currently in scope
- Find an issue that is security related
- Properly document the security vulnerability by creating a JIRA issue within the "[hack.dt](#)" project
  - Meaningful JIRA issue title
  - Set label to *BugBounty\_Q12018*
  - Describe the issue environment as detailed as possible
  - Describe how you found the issue
  - Attach a working proof of concept on how to reproduce the finding (including screenshots or videos)
- Assign the issue to [@Schulz, Pascal](#)


After the issue has been created, the bug bounty supervisor and his board of reviewers will check all issues for eligibility. A created issue only counts as valid submission if all above mentioned steps are fulfilled.

# Bug Bounty Program


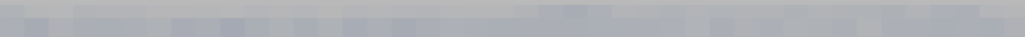

Created by Schulz, Pascal, last modified on Mar 30, 2018

## Who can participate in the bug bounty program?

- P
- S
- R
- P
- P

Bug Bounty Season	Vulnerability Overview	Vulnerability Statistics (fixed / found)
Hack.DT Season 1.0	Hack.DT Season 1.0	<div> <div>HIGH</div> <div>MEDIUM</div> <div>LOW</div> <div>INFO</div> <div>TOTAL</div> </div> 
2018-01-18 to 2018-02-28		
Budget: \$ 20.000		
JIRA label: BugBounty_Q12018		

## → Findings

Test Environment	SaaS: 
	Managed: 
Ticket to book time	 APM-118291 <span>OPEN</span>
Primary Contact	<span>@Schulz, Pascal</span>



# What could we have done better?

---

Disclaimer: Similarities to traditional Penetration Tests are given

# Triaging of findings stated huge effort for bug bounty supervisory board



**Poor issue description quality  
(due to lack of security know-how)**

---



# Lack of working POCs

---





**CVSS score not always suitable**  
**(not always quite clear which option to choose in**  
**score calculator)**

---



# Sensitive Information Disclosure

---



**Difficult to differentiate attack payloads  
if same staging system is used for everyone**



**Difficult to check reward eligibility  
(had finding been existing before)**





**Some findings targeted features  
in active development  
(should be excluded from scope)**

---



# **Advantages of running an internal over an external bug bounty program**

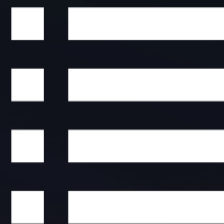
---

# Raise employee awareness

---



# Receive insights into security grey areas (broader scope)





# Higher number of findings compared to external tests

- 
- 1 ☐
  - 2 ☐
  - 3 ☐
  - 4 ☐

# Excellent cost per finding ratio

---




# How to raise awareness?

---

# Share Results

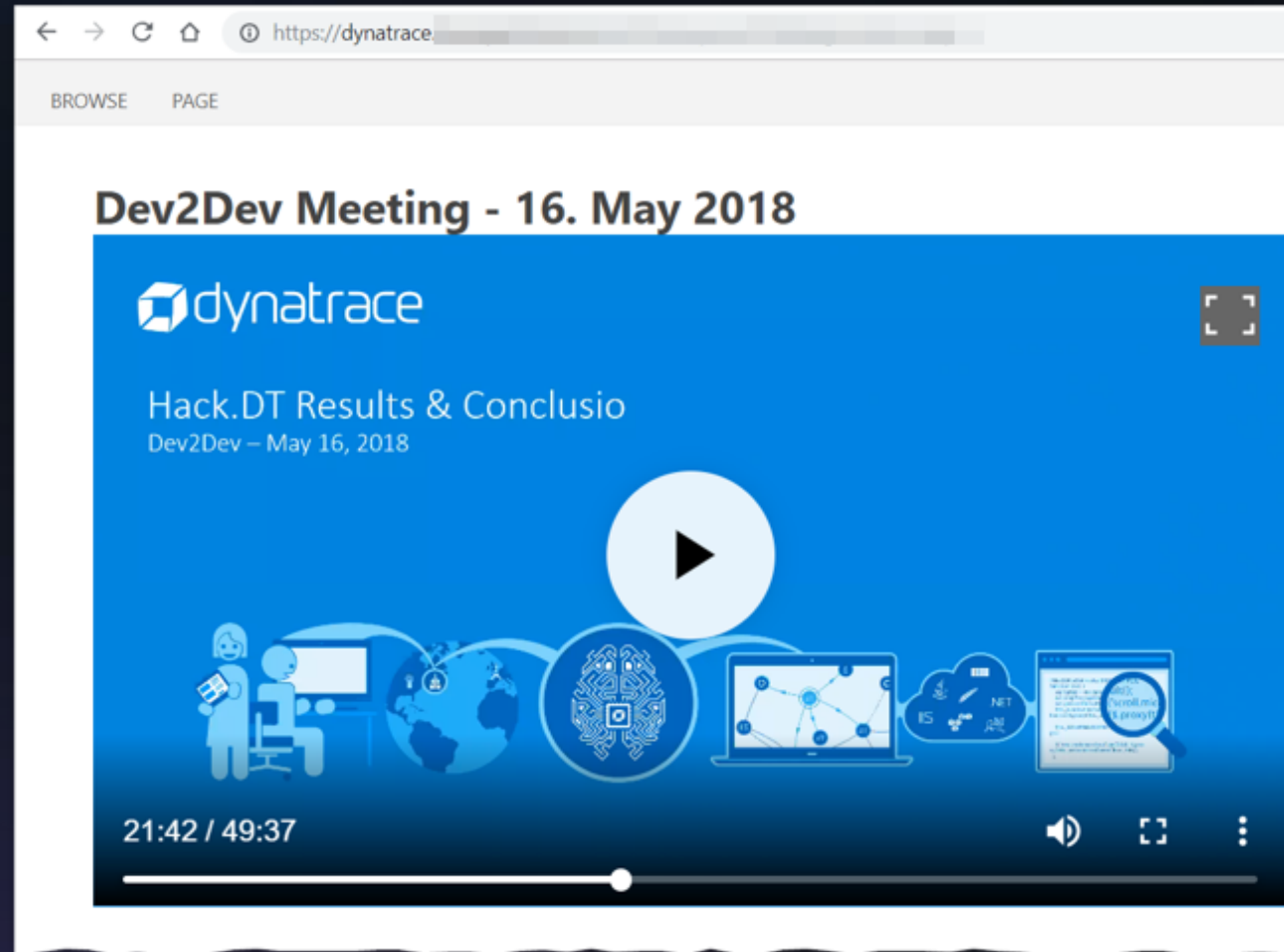
	Hacker	Vulnerability	CVSS Score	Reward	Payment State
1	 Yury	 APM-118243 RESOLVED	6.4	\$ 320	submitted
2	 Stefan	 APM-118252 RESOLVED	5.3	\$ 265	submitted
3	 Stefan	 APM-118255 RESOLVED	5.3	\$ 265	submitted
4	 Daniel	 APM-118279 RESOLVED	5.1	\$ 255	submitted
5	 Daniel	 APM-118280 RESOLVED	5.3*	\$ 133*	submitted
6	 Stefan	 APM-118283 RESOLVED	5.3	\$ 265	submitted
7	 Stefan	 APM-118289 RESOLVED	5.3	\$ 265	submitted
8	 Stefan	 APM-118338 RESOLVED	3.7 6.7	\$ 428	submitted
9	 Christian	 APM-118351 RESOLVED	5.3	\$ 265	submitted



	Hacker	Total Reward	February	March
1	 Daniel	\$ 2.475	\$ 2.475	
2	 Stefan	\$ 1.933	\$ 1.703	\$ 230
3	 Josef	\$ 1.353	\$ 815	\$ 538
4	 Ludwig	\$ 1.008	\$ 408	\$ 600



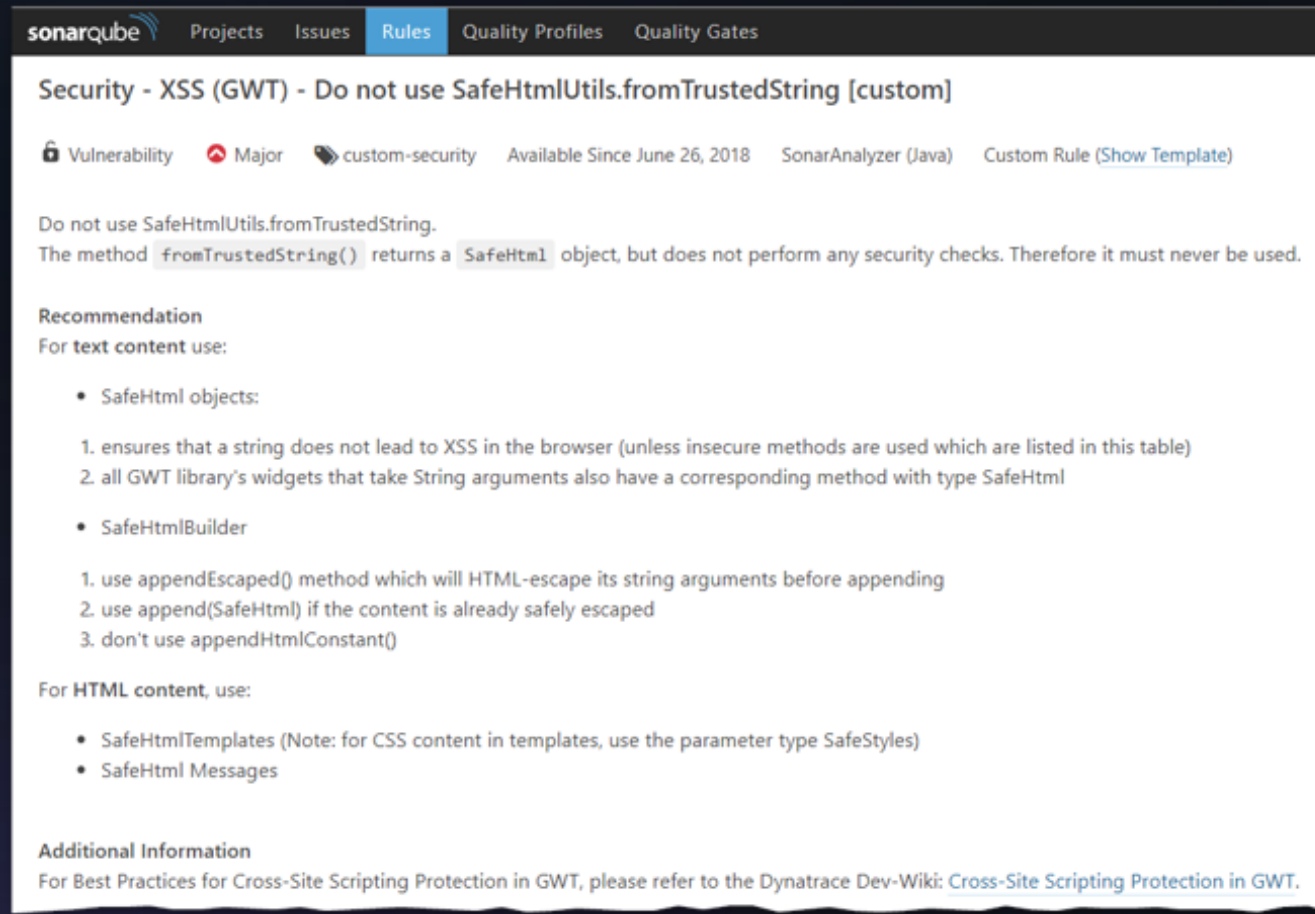
# Present Findings



# Create Security Awareness Training

The screenshot displays the user interface for the 'Dynatrace 2018 Security Awareness Training' course. At the top, a navigation bar includes the Dynatrace logo, a 'Categories' menu, a search bar labeled 'Search for Courses', and links for 'Create a Course', 'My Courses', and a user profile icon labeled 'PS'. The main header area features the Dynatrace logo on the left and the course title 'Dynatrace 2018 Security Awareness Training' on the right. Below the title, there is a red button labeled 'Continue to Lecture 1', a five-star rating system with the text 'Edit Your Rating', and a progress indicator showing '9 of 9 items complete' with a corresponding progress bar and a trophy icon. A secondary navigation bar contains tabs for 'Overview', 'Course Content' (which is selected), 'Q&A', 'Bookmarks', 'Announcements', and 'Options'. Below this, a search bar for 'Search course content' is present, along with links for 'Current Section', 'All Sections', and 'All Resources'. The 'Section: 1' header is followed by the 'Introduction' section. A list of items under this section includes '1. Introduction' (highlighted in teal with a play button icon, a duration of '1:16', and a refresh icon) and 'Security Website' (indicated by a link icon).

# Introduce SAST Rules



The screenshot shows the SonarQube interface with the 'Rules' tab selected. The rule title is 'Security - XSS (GWT) - Do not use SafeHtmlUtils.fromTrustedString [custom]'. It is categorized as 'Vulnerability' (lock icon), 'Major' (red triangle icon), and 'custom-security' (wrench icon). It was available since June 26, 2018, for SonarAnalyzer (Java), and is a custom rule with a 'Show Template' link.

**Do not use SafeHtmlUtils.fromTrustedString.**  
The method `fromTrustedString()` returns a `SafeHtml` object, but does not perform any security checks. Therefore it must never be used.

**Recommendation**  
For **text content** use:

- **SafeHtml objects:**
  1. ensures that a string does not lead to XSS in the browser (unless insecure methods are used which are listed in this table)
  2. all GWT library's widgets that take `String` arguments also have a corresponding method with type `SafeHtml`
- **SafeHtmlBuilder**
  1. use `appendEscaped()` method which will HTML-escape its string arguments before appending
  2. use `append(SafeHtml)` if the content is already safely escaped
  3. don't use `appendHtmlConstant()`

For **HTML content**, use:

- **SafeHtmlTemplates** (Note: for CSS content in templates, use the parameter type `SafeStyles`)
- **SafeHtml Messages**

**Additional Information**  
For Best Practices for Cross-Site Scripting Protection in GWT, please refer to the Dynatrace Dev-Wiki: [Cross-Site Scripting Protection in GWT](#).

# Basic cost overview

---



## Hackerone

Annual Fee:	\$ 36.000
Bounty Budget:	\$ 20.000
Total:	\$ 56.000



## Synack

Annual Fee:	€ 145.000
Bounty Budget:	€ 0
Total:	€ 145.000



## Bugcrowd

Annual Fee:	\$ 36.000
Bounty Budget:	\$ 20.000
Total:	\$ 56.000



## Dynatrace

Employees:	\$ 37.000
Bounty Budget:	\$ 20.000
Total:	\$ 57.000





# Find out more about the program

---



Blog

<https://www.dynatrace.com/news/blog/running-a-successful-internal-bug-bounty-program/>



Podcast

<https://www.spreaker.com/user/pureperformance/065-running-a-successful-internal-bug-bo>





Questions?

Feedback?

Please contact me via [pascal.schulz\[at\]dynatrace.com](mailto:pascal.schulz@dynatrace.com)





**Get ready to be amazed**  
in 5 minutes or less

[dynatrace.com/trial](https://dynatrace.com/trial)





[dynatrace.com](https://dynatrace.com)