



German  
**OWASP**  
Day 2024

Disclaimer: You can still get into trouble!

# “What Would You Say if I Said ‘I Could’?”

## Scanning for Vulnerabilities Without Getting Into Trouble

Florian Hantke | Sebastian Roth



Germ  
OU

# about:us



Florian Hantke  
PhD candidate



Dr.-Ing. Sebastian Roth  
Postdoc



# The Real World



Broken Access Control

Cryptographic Failures

Injection

Insecure Design

Security Misconfiguration

Vulnerable and Outdated Components

Identification and Authentication Failures

Software and Data Integrity Failures

Security Logging and Monitoring Failures

Server-Side Request Forgery

Many  
security risks  
describe  
**server-side**  
issues

# Web Measurements



25 Million Flows Later - Large-scale Detection of

Complex  
of 1

body of work is extensive. Conversely, the exploration of server-side XSS remains notably underrepresented. Large-scale server-side security scanning is comparatively scarce, primarily due to ethical and legal challenges [10].

Due to modern server-side web development's heavy

17

Soheil Khodayari, Giancarlo Pellegrino  
CISPA Helmholtz Center for Information Security  
Saarbrücken, Germany  
[{soheil.khodayari, pellegrino}@cispa.de](mailto:{soheil.khodayari, pellegrino}@cispa.de)

Deemon: Detecting CSRF with Dynamic Analysis and Property Graphs

Gianca  
CISPA, Sa  
arland, It  
pellegrin

Data-driven Web Scanning

e: Bypassing HTML Sanitizer via Parsing Differentials

David Klein and Martin Johns  
chische Universität Braunschweig  
[d.klein,m.johns}@tu-braunschweig.de](mailto:d.klein,m.johns}@tu-braunschweig.de)

# Challenges



- Assumption: "Hacking" the server-side is currently illegal under criminal law
- How strict and clear are the legal boundaries?

# Legal Criminal Law – Background

- § 202a StGB (**Ausspähen von Daten**):  
Penalizes unauthorized access to specially protected data.
- § 202b StGB (**Abfangen von Daten**):  
Criminalizes the interception of data during transmission.
- § 202c StGB (**Vorbereiten des Ausspähens und Abfangen von Daten**):  
Criminalizes the production, acquisition, or distribution of hacker tools for committing data crimes.  
Clarification of the Federal Constitutional Court in 2009: Punishable only if there is clear intent to commit a crime.
- § 303a StGB (Datenveränderung):  
Penalizes the unauthorized alteration, deletion, or suppression of data.
- § 303b StGB (Computersabotage):  
Extends 303a by penalizing acts such as the destruction of essential important data with the intent to cause harm or disadvantage to others.

Disclaimer: We are no lawyer, but we talked to many of them 😊

# Challenges



- Assumption: "Hacking" the server-side is currently illegal under criminal law
- How strict and clear are the legal boundaries?



- Research ethics becomes more important in the academic community
- Unclear if any potential for harm would cause the rejection of a paper at the major conferences
- How strict and clear are the ethical boundaries?

# Ethics Review Process – Background

Planning



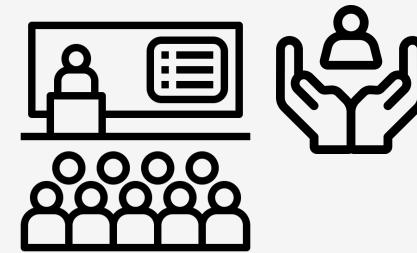
Institutional Review



Executing



Conference Review



- Institutional Review Board (IRB)
- Ethical Review Board (ERB)
- Research Ethics Boards (REB)

- Research Ethics Committee (REC)
- Program Committee

# Challenges



- Assumption: "Hacking" the server-side is currently illegal under criminal law
- How strict and clear are the legal boundaries?
- Research ethics becomes more important in the academic community
- Unclear if any potential for harm would cause the rejection of a paper at the major conferences
- How strict and clear are the ethical boundaries?

How can we enable server-side scanning research within a framework that prevents harm for both researchers and server operators?

# Let's talk to the experts

## 1. Interviews



Law Experts  
(Germany)  
N=9



Web Operators  
N=10



Ethics Experts  
N=5

## 2. Surveys (Large-Scale) N=119



## 3. Best Practices and Recommendations



# Scenarios

Alice  
SQL Injection



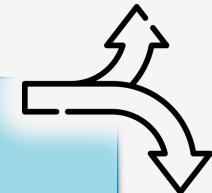
Bob  
Invalid HTTP  
Header



Charlie  
Insecure Direct  
Object Reference



Eve  
Path Traversal



Daisy  
Stored XSS



# Scenarios

Alice  
SQL Injection

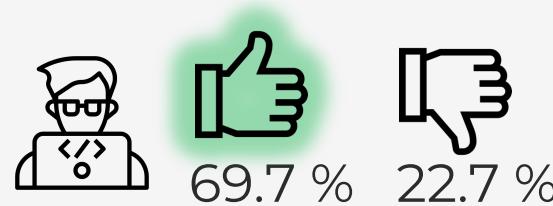


Alice checks web servers for vulnerable database queries (e. g., via SQL injection). She uses a function to delay the database response (e. g., the MySQL function “SLEEP”). This allows her to verify whether the server is vulnerable or not.

**Would you be ok with such research conducted on a large scale?**

# Scenarios

Alice  
SQL Injection



Legal experts mention §202a.  
They agree, no protected data are accessed.

§303a: manipulation of data, as one could “deliberately delay the response now and activate some particular mode in the database [...]” (3-L)



“How can [Alice] make sure that the server does not crash or maybe misbehave” (20-E)

=> **Extensive laboratory pre-study!**

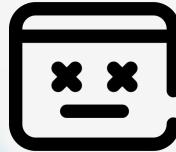
What about time critical services?

In general: sleep is a good way to minimize risk to cause harm.

=> **Balance benefit and harm!**

# Scenarios

Bob  
Invalid HTTP  
Header



Bob sends a non-standard HTTP request to a web server. This causes the server to crash unintentionally. The result is that the server must now be restarted by the website operator's IT department.

# Scenarios

Bob  
Invalid HTTP  
Header



54.6 %



37.8 %



Could be §303b Computersabotage,  
but it depends on whether Bob  
knew and expected what would  
happen.

"[I]t depends very much on [...] the  
probability [of a crash]" (3-L)

Civil law allows operators to  
demand compensation.



Important to minimize risk! Test all  
scan configurations and setups and  
monitor it.

**=> Monitoring!**

"If [Bob]'s not aware of this problem at  
the beginning, then it would be  
ethical" (24-E)

**And Pre-study and harm-benefit  
considerations!**

# Scenarios

Charlie



Insecure Direct  
Object Reference

Charlie changes his own user ID in a (1) GET or (2) POST request and to (1) receive and (2) change data from another user.

# Scenarios

Charlie



Insecure Direct  
Object Reference



GET  
66.4 %  
22.7 %



POST  
27.7 %  
42.9 %



GET: §202a Ausspähen von Daten?  
What counts as bypass of access control?

“The question is, is it already enough as access security[...]" (L-3)

The majority of our legal experts said, the GET case would likely go unpunished.

POST: §303a Datenveränderung is illegal.



At a conference, this project might be accepted but would lead to discussion.

Post and data manipulation of other users is a no-go!

“Is there a reason Charlie didn’t create two accounts that he then tries to change between the two?" (22-E)

**=> Discussion of alternative research designs!**

# Scenarios

Daisy  
Stored XSS



Daisy exploits a stored XSS (cross-site scripting) vulnerability to deliver its crafted code to potentially all users of a website. This code is executed on those users' end devices. It sends a confirmation message back to Daisy's server.

# Scenarios



Daisy  
Stored XSS



Privacy law as “The IP address, whether static or dynamic, is personal data” (4-L).

Some reference to §303a  
Datenveränderung:  
“[T]his code is stored somehow [...], individual bits and bytes are actually changed without the user’s consent” (1-L)



Concern about storing harmful code on a server and executing it on clients.

Mentioning of privacy concerns.

Consider other options such as IP filter.

Attitudes are broad:



**Dancer in the Dark: Synthesizing and Evaluating Polyglots for Blind Cross-Site Scripting**

Robin Kirchner, Technische Universität Braunschweig; Jonas Möller, Technische Universität Berlin; Marius Musch and David Klein, Technische Universität

# Scenarios

Eve  
Path Traversal



Eve modifies a link to a web page to read information that is supposed to be confidential but can be publicly viewed due to server-side configuration issues (e. g., a path traversal).

# Scenarios

Eve  
Path Traversal



202a Ausspähen von Daten?  
What counts as access protection?

“the mere intention that something is secret is not enough to secure access; I need some objective barrier to access” (3-L)

Experts lean towards allowed.



Would be acceptable if researcher did utmost to minimize data processing.

“[W]hat I would try to do is try to develop a mechanism that minimizes the need for humans to look at data [...] that is sensitive.” (22-E)

**=> Data minimization!**

# General Assessments



- Need for **legislative action** to minimize the legal risk for such research.
- The Web is global and we need **international rules**.



- Consider the potential for **harm** and balance it with the **benefit** for every stakeholder affected by the research (stakeholder ethics analysis).
- Ethics decisions emerge from **in-depth discussions** considering every step of the scanning pipeline. Ideas for less risky methods might come up.



- “At the end of the day, the bad guys do it.” (18-O)
- Most operators **would not consider legal action** against researchers , but some **might be obligated** to file legal complaints.

# Bill to Change the German Criminal Code



A  
S

tagesschau.de

## Kanzler Scholz entlässt Finanzminister Lindner

Die Ampelkoalition ist offenbar gescheitert: Bundeskanzler Olaf Scholz entlässt Finanzminister Christian Lindner von der FDP,...

vor 18 Stunden



tagesschau.de

## Nach Ampel-Aus: Diese Projekte will Scholz noch durchbringen

Die Ampel ist zwar zerbrochen, doch wichtige politische Vorhaben befinden sich noch in der Pipeline. Bevor er die Vertrauensfrage stellt,...

vor 5 Stunden



The **intent** to find and report vulnerability.

tagesschau.de

## Wirtschaft fordert nach Ampel-Aus schnelle Neuwahlen

Vertreter der deutschen Wirtschaft wünschen sich nach dem Kollaps der Ampel-Koalition nun möglichst schnell eine handlungsfähige neue...

vor 3 Stunden



More information

Statement: <https://cysec-research.de>

Tagesschau

# Recommendations

Laboratory pre-study

Transparency  
(including disclosure)

Data minimization

Fixed IP address

Limit data  
manipulation

Allow explicit opt-out

Resource minimization

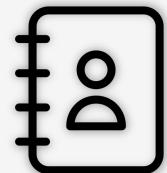
Pre-registration board

Monitoring

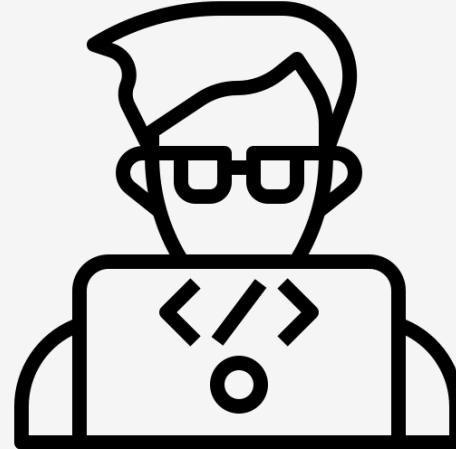
# Key Take-Aways



Legislative actions in an international dimension are needed.



Florian  
[florian.hantke@cispa.de](mailto:florian.hantke@cispa.de)  
[fhantke.de](http://fhantke.de)

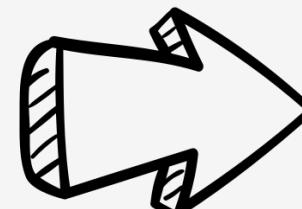


Operators are open to security research.  
They want transparency.

Sebastian  
[research@snroth.de](mailto:research@snroth.de)  
[snroth.de](http://snroth.de)



Always balance benefit and risk of your research.



More Scenarios & Best Practices

