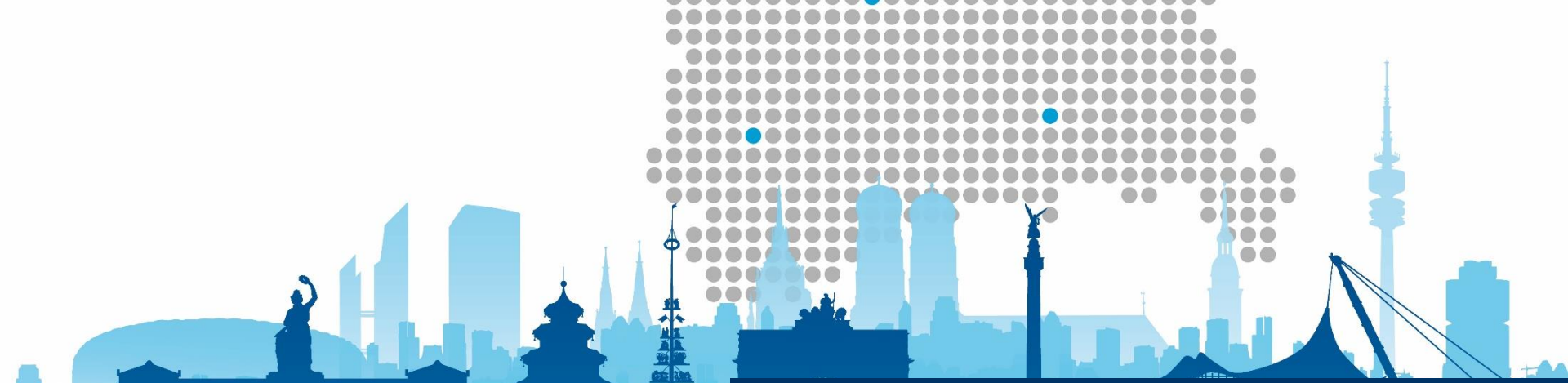


IHK-BugBounty Programm

Warum, Wieso, Weshalb…

IHK

Mail an die IHK

>>> Rajosh …<…@gmail.com>

Hi Team,

I am a Security Researcher and have found a couple of *Security Vulnerability (Reflected-XSS)* on your website: https://www.....de/

Could you please share the details of your *Development Team / Security Team* or forward this mail to them?

Also, I wanted to check if you have a *Bug Bounty/Responsible Disclosure Program* where I can report this issue.

Reference:

https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

Thanks in advance.

Best Regards,

Rajosh

Mail an die IHK

Please support the OWASP mission to improve software security through open source initiatives and community education. Donate Now!

OWASP PROJECTS CHAPTERS EVENTS ABOUT Member Login Store Donate Join

OWASP Top Ten 2017

A7:2017-Cross-Site Scripting (XSS)

Languages: [en] de

← A6:2017-Security Misconfiguration | OWASP Top Ten 2017 PDF version | A8:2017-Insecure Deserialization →

Threat Agents / Attack Vectors		Security Weakness		Impacts	
App. Specific	Exploitability: 3	Prevalence: 3	Detectability: 3	Technical: 2	Business ?
Automated tools can detect and exploit all three forms of XSS, and there are freely available exploitation frameworks.		XSS is the second most prevalent issue in the OWASP Top 10, and is found in around two thirds of all applications. Automated tools can find some XSS problems automatically, particularly in mature technologies such as PHP, J2EE / JSP, and ASP.NET.		The impact of XSS is moderate for reflected and DOM XSS, and severe for stored XSS, with remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.	

Is the Application Vulnerable?

There are three forms of XSS, usually targeting users' browsers:

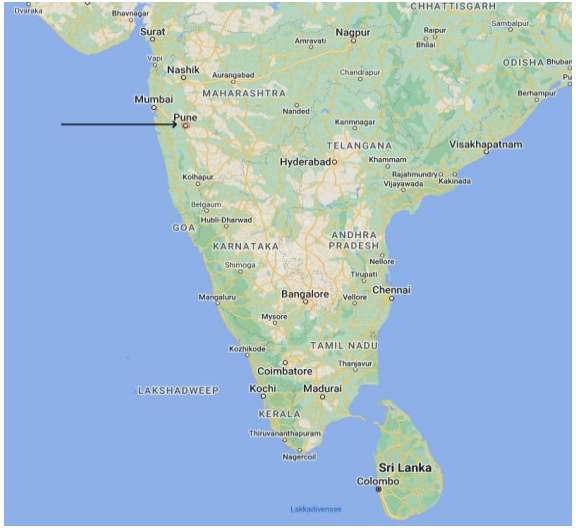
* **Reflected XSS**: The application or API includes unvalidated and unescaped user input as part of HTML output. A successful attack can allow the attacker to execute arbitrary HTML and JavaScript in the victim's browser. Typically the user will need to interact with some malicious link that points to an attacker-controlled page, such as malicious watering hole websites, advertisements, or similar.
* **Stored XSS**: The application or API stores unsanitized user input that is viewed at a later

How to Prevent

Preventing XSS requires separation of untrusted data from active browser content. This can be achieved by:

* Using frameworks that automatically escape XSS by design, such as the latest Ruby on Rails, React JS. Learn the limitations of each framework's XSS protection and appropriately handle the use cases which are not covered.
* Escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) will resolve Reflected and Stored XSS vulnerabilities.

Mail an die IHK



Infoquelle: LinkedIn

- Pune, Maharashtra, India
- Seit 8 Jahren angestellt bei A.
  Dt. Niederlassung: A… GmbH, Giesing

1. IHK-BugBounty Programm

IHK-Website:

- Hinweise auf Schwachstellen: IHK-BugBounty-Programm https://www.ihk-muenchen.de -> „Über Uns“ -> „Hinweise auf Schwachstellen: IHK-BugBounty-Programm“
- Indications of Vulnerabilities: CCI BugBounty Program

1. Was ist das IHK-BugBounty Programm?
2. Welche digitalen Services umfasst das BugBounty Programm?
3. Regeln für das das BugBounty Programm!
4. So können Sie uns eine Schwachstellen-Meldung zukommen lassen
5. Was tut die IHK mit Meldungen von Schwachstellen?

Muster: BugBounty-Programm
https://www.ihk-muenchen.de → Ratgeber → Digitalisierung → Informationssicherheit

1. Was ist das, ein BugBounty-Programm?
2. Ist ein BugBounty-Programm für mein Unternehmen sinnvoll?
3. Ein eigenes BugBounty-Programm planen
4. Muster: Word-Dokument und dessen Verwendung
5. Muster: BugBounty-Programm
6. Beispiele für Schwachstellenmeldungen

2. Welche digitalen Services umfasst das BugBounty Programm?

„Folgende Domains (inkl. ggf. vorhandener Subdomains) sind relevant für das BugBounty Programm der IHK für München und Oberbayern:

- ausbilderfit.de
- …
- uehi.de“

„Bitte beachten Sie, dass nicht in der obigen Liste enthalte digitale Services nicht Teil des BugBounty Programms sind. Ggf. kann eine IT-Sicherheitsuntersuchung solcher nicht genannter Services als rechtswidrig eingestuft und entsprechend geahndet werden.“

Effekt: Wir bekommen auch Schwachstelleninfos für andere IHKs….

3. Regeln für das das BugBounty Programm!

- Schaden darf nicht entstehen, z. B.:
  „Bitte führen Sie daher keine Phishing-Mail-, DDoS-, Brute-Force-Tests o. ä. durch. Ändern Sie keine Daten.“

- „Aktuelle und ehemalige Mitarbeiter der IHK für München und Oberbayern sowie Dienstleister und Zulieferer können nicht am BugBounty Programm teilnehmen.“

4. So können Sie uns eine Schwachstellen-Meldung zukommen lassen

bugbounty@muenchen.ihk.de

Inhalt:

- Exakte Domain, auf welcher die Schwachstelle gefunden wurde
- Möglichst viele Details zur Reproduktion der Schwachstelle, um uns die Analyse zu erleichtern und damit die Auszahlung der Belohnung zu beschleunigen.
  Z. B. IP-Nummer von der aus getestet wurde, Proof-Of-Concept-Skizzen.

Veröffentlichen ist das eine….

Etwas anderes ist es…
…eingehende Meldungen wahrnehmen, bewerten, Entscheidungen zutreffen….

5. Was tut die IHK mit Meldungen von Schwachstellen?

Schwachstelle-Einordnung	Niedrig	Mittel	Hoch	Kritisch
CVSS-Score	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0
BugBounty (Nettobetrag vor Umsatzversteuerung)	bis 100 €	100 – 500 €	500 – 1.000 €	über 1.000 €

CVSS: Common Vulnerability Scoring System Calculator

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

https://www.cve.org

Bewertung einer Schwachstelle von 0 bis 10

Beispiel: „Schwachstelle mit hoher Gefährdung der Vertraulichkeit, die übers Internet ohne besondere Kenntnisse und Rechte, direkt vom Angreifer durchgeführt werden kann“ → 7.5

Wenn zusätzlich auch die Verfügbarkeit gefährdet ist → 9.1

Wenn die Schwachstelle kompliziert ist und man bestimmte Rechte auf dem IT-System benötigt, sinkt der Wert → 6.8

→ Wichtig für BugBounty, aber vor Allem für Updates!!

Rechnung, Zahlungswege…

Wie kommt der BugHunter zu seiner Belohnung?

Kommt darauf an:

- Gewerblich tätig?
- Mehrwertsteuer?
- Rechnung möglich?

Konkret:

- Student aus den USA
- Privatperson aus Deutschland
- Unternehmen aus der EU
- …