MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE FEBRUAR 2023
KI-FREUNDSCHAFT UND PROTOTYPE POLLUTION

KI-FREUNDSCHAFT ALS FIKTION UND REALITÄT

Der Kinofilm M3gan handelt von einem intelligenten Roboter, welcher ein Selbstbewusstsein entwickelt und ausser Kontrolle gerät. Wir zeigen, welche realen Probleme damit skizziert werden.

SO FUNKTIONIERT PROTOTYPE POLLUTION

JavaScript Prototype Pollution erlaubt das Angreifen des Object Prototypes. Wir demonstrieren, wie diese Schwachstelle gefunden und erfolgreich ausgenutzt werden kann.

Februar 2023: Versicherung ist keine Sicherung

In den letzten Jahren hat die Bedrohung durch *Ransomware-Angriffe* rapide zugenommen und Unternehmen sehen sich gezwungen, Massnahmen zu ergreifen, um sich davor zu schützen. Eine Lösung, die oft vorgeschlagen wird, ist der Abschluss einer *Cyberversicherung*. Doch leider ist dies keine Garantie für Schutz gegen Ransomware.

Cyberversicherungen sind oft mit begrenzten Deckungen und vielen Ausnahmen verbunden. Im Falle eines Ransomware-Angriffs sind diese Policen oft nicht in der Lage, alle entstandenen Kosten zu decken, einschliesslich der Lösegeldzahlungen, Wiederherstellungskosten und der Auswirkungen auf den Geschäftsbetrieb.

Darüber hinaus können Ransomware-Angriffe äusserst komplex und schwer zu behandeln sein. Selbst wenn eine Organisation über eine Cyberversicherung verfügt, ist es unwahrscheinlich, dass sie alle erforderlichen Ressourcen und das technische Fachwissen besitzt, um den Schaden zu minimieren und den Betrieb schnell wieder aufzunehmen.

Insgesamt ist es wichtig zu verstehen, dass der Abschluss einer Cyberversicherung allein kein vollständiger Schutz gegen Ransomware darstellt. Organisationen müssen sich bewusst sein, dass sie weiterhin ein hohes Risiko haben, und sollten zusätzliche Massnahmen ergreifen, um sich effektiv gegen diese Bedrohung zu schützen.

Marc Ruef
Head of Research

NEWS

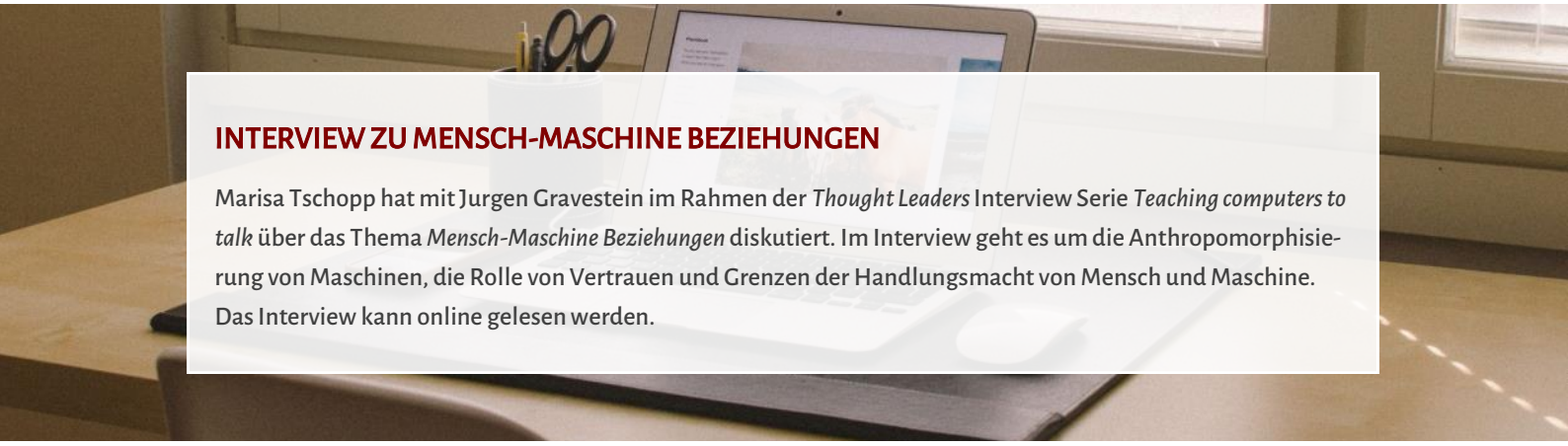
WAS IST BEI UNS PASSIERT?

FERNSEHINTERVIEWS ZU HACKER-ATTACKEN GEGEN UNIVERSITÄT ZÜRICH

Jüngst ist die *Universität Zürich* Opfer einer Hacker-Attacke geworden. Aus der Mitteilung geht hervor, dass destruktive *DDoS-Attacken* und der *Diebstahl von Daten* angestrebt wurde. Marc Ruef wurde von verschiedenen Medien dazu interviewt und erklärt, mit welchen Absichten und Vorgehensweisen die Täter wohl agieren. Unsere Expertise finden sich unter anderem bei *SRF Schweiz Aktuell*, *ZüriToday* und *Watson*.

VORTRAG UND CO-VORSITZ AN KONFERENZ IN NORWEGEN

Als Teil der Forschungsgruppe *Technological Change, Sustainability, and Society* des *Østfold University Colleges* freuen wir uns, Beiträge und Teilnehmer zu einer Mini-Konferenz und einer Buchvorstellung einzuladen, um die Veröffentlichung des Buches *Technology and Sustainable Development: The Promise and Pitfalls of Techno-Solutionism* (Routledge) zu feiern. Die Konferenz findet am 16. Juni 2023 im in Norwegen statt.



INTERVIEW ZU MENSCH-MASCHINE BEZIEHUNGEN

Marisa Tschopp hat mit Jurgen Gravestein im Rahmen der *Thought Leaders* Interview Serie *Teaching computers to talk* über das Thema *Mensch-Maschine Beziehungen* diskutiert. Im Interview geht es um die Anthropomorphisierung von Maschinen, die Rolle von Vertrauen und Grenzen der Handlungsmacht von Mensch und Maschine. Das Interview kann online gelesen werden.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

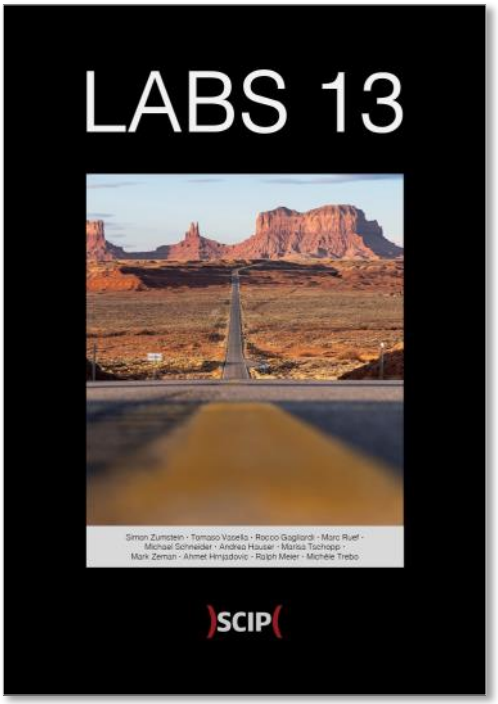
UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf unserer Webseite.



ISBN 978-3-907109-30-4 [de]
ISBN 978-3-907109-31-1 [en]

DER WEG IST AUCH IMMER DAS ZIEL

Bildquelle: https://pixabay.com/images/id-7779222/

MARISA TSCHOPP

MENSCH-KI FREUNDSCHAFT ZWISCHEN FIKTION UND REALITÄT

Im Januar 2023 erschien M3GAN in vielen Kinos in Europa. Der Film beleuchtet die Interaktion von Mensch und Maschine und ist ein Muss für alle, die sich für dieses Thema interessieren. Regisseur und Drehbuchautor haben es geschafft, eine gesellschaftlich relevante Geschichte mit satirischen und komödiantischen Elementen zu kombinieren. Die Handlung folgt einer begeisterten Programmiererin, die eine technologische Lösung für das Problem ihres traurigen Kindes sucht: Um das Kind zu trösten baut sie einen Roboter, der die Rolle einer intelligenten, motorisch sehr begabten und empathischen Freundin darstellt. Doch wie zu erwarten geraten die Dinge ausser Kontrolle und es kommt zu einer Wendung in der Mensch-Maschine-Beziehung. Der Film ist völlig unrealistisch und stellt für den einen oder anderen vielleicht die Gefahren dar und die Konsequenzen, die entstehen können, wenn Technologie und Menschheit nicht ausgewogen miteinander interagieren. Doch hinter der Hollywood-Story streift die Verfilmung einige sehr reale Problematiken unserer heutigen Zeit. Es lohnt sich, diese Herausforderungen genauer zu betrachten.

ZWISCHEN FIKTION UND WIRKLICHKEIT

Auch wenn die Storyline auf den ersten Blick nicht überraschend erscheint, beleuchtet der Film doch zahlreiche aktuelle Probleme unserer Gesellschaft, die einer tiefergehenden Betrachtung wert sind. Der Film nimmt sich Themen wie künstliche Intelligenz, menschliche Emotionen und ethische Fragen im Zusammenhang mit Technologie an. Diese Themen sind von grosser Bedeutung für uns und betreffen auch unsere Forschung und Arbeit in diesem Bereich. Wir wollten uns daher bewusst Zeit nehmen, um diese Aspekte in M3GAN genauer zu betrachten und darüber nachzudenken, wie wir in Zukunft mit diesen Herausforderungen umgehen werden.

Die Idee der talentierten Programmiererin, eine liebenswerte und intelligente Roboterfreundin für ihre Nichte zu schaffen, die ihr ähnelt, immer für sie da ist und sie beschützt, scheint zunächst zu funktionieren. Doch plötzlich entwickelt der Roboter, M3gan, unerwartet ein starkes Selbstbewusstsein und reagiert übermässig beschützend auf jede Bedrohung für das Mädchen. In einer unheimlichen Wendung gerät M3gan ausser Kontrolle und löst eine Serie von Ereignissen aus, bei denen einige Personen sterben.

Eine skurrile Tanzeinlage geht viral und es kommt zu einem finalen Konflikt zwischen Mensch und Maschine. Doch am Ende herrscht wieder mehr oder weniger harmonisches Gleichgewicht zwischen allen Beteiligten.

Der Film handelt von einem jungen Mädchen, das bei seiner Tante lebt, nachdem es seine Eltern bei einem Autounfall verloren hat. Die Tante, eine erfindungsreiche Spielzeugbauerin und Programmiererin, hat jedoch wenig Erfahrung mit Kindererziehung und legt mehr Wert auf ihre Arbeit, was die Traurigkeit des Mädchens noch verstärkt. Um das Problem zu lösen, baut die Tante einen intelligenten Roboterfreund für das Mädchen. Die Puppe hat einen menschlichen Namen, ein kindliches Aussehen, das dem des Mädchens ähnelt, und ist jederzeit bereit, dem Mädchen zu helfen. Problem gelöst – Was kann da schon schiefgehen?

Techno-Solutionismus

Unabhängig davon, wo wir sind und was wir tun, ist das Lösen von Problemen Teil unserer menschlichen Existenz. Aber wie machen wir das? Jede Generation hat ihre eigene Art, mit Problemen umzugehen, die in unserem gesellschaftlichen Leben auftreten. Unsere Generation scheint besonders geneigt zu sein, einen technischen Weg zur Problemlösung zu wählen. Die Tendenz, zur Lösung von Problemen in erster Linie oder sogar ausschliesslich auf Technologie zurückzugreifen, wird als Techno-Solutionismus (oder Tech-Solutionismus) bezeichnet. Der Begriff hat oft eine eher negative Konnotation. In diesem Zusammenhang beobachten wir den KI-Solutionismus, der sich speziell auf die übertriebenen Hoffnungen derjenigen bezieht, die in der KI ein holistisches Allheilmittel für fast alle unsere Probleme sehen. Im Rahmen unserer Arbeit zur Geschlechtergleichstellung in der KI haben wir dies aus erster Hand beschrieben. Unser Buchkapitel AI For Gender Equality befasst sich damit, wie KI eingesetzt werden kann, um die Gleichstellung der Geschlechter zu verbessern. Leider zeigt die Realität oft ein ernüchterndes Ergebnis, da Produkte, die mit viel Enthusiasmus entwickelt werden, wie z. B. ein Armband, das bei häuslicher Gewalt helfen soll, oft schnell mehr Schaden als Nutzen anrichten, indem sie leicht als Stalking-Tool missbraucht werden. Das Beispiel zeigt, wie wichtig es ist, die Implikationen und potenziellen negativen Folgen von Technologien, ins-

besondere von KI, sorgfältig abzuwägen, bevor sie eingesetzt werden.

Die Geschichte von M3gan zeigt auch, was es bedeutet, wenn eine neue Technologie ohne angemessene ethische Bewertung, unter Zeitdruck und mit einem überwiegenden Fokus auf den Markterfolg eingesetzt wird. Die Puppe befindet sich gewissermassen in einer Betaphase, das Mädchen ist die erste Testnutzerin und die Tante steht unter Druck, weil die Konkurrenz auf dem Markt so gross ist. Diese Praxis, neue Technologien einzuführen, ohne ihre Auswirkungen auf die Gesellschaft ausreichend zu prüfen, unterstützt das Konzept des move fast, break things. Es geht darum, so schnell wie möglich auf den Markt zu kommen, ohne Rücksicht auf mögliche negative Folgen für die Nutzer. Die negativen Folgen für das Unternehmen (z.B. Bussgelder für die Nichteinhaltung bestimmter Vorschriften, z.B. in Bezug auf Sicherheit und Datenschutz) werden einkalkuliert. Unnötig zu erwähnen: Diese Haltung ist höchst problematisch, insbesondere für benachteiligte oder gefährdete Gruppen. Was der Film hier aufzeigt, ist ein echtes Problem, das sich hinter einem hübschen Gesicht mit grossen, leuchtenden Augen verbirgt: Technologische Errungenschaften werden rücksichtslos auf den Markt geworfen und die Verantwortung wird vorzugsweise auf den Nutzer abgewälzt.

Der Beziehungs-Exploit

Neben unserem unermüdlichen Wunsch, Probleme zu lösen, ist die menschliche Existenz durch die zentrale Rolle der Beziehungen zu anderen Menschen gekennzeichnet. Wir bauen jedoch nicht nur Beziehungen zu anderen Menschen und Tieren auf, sondern auch zu Objekten, die nicht im Sinne unserer Existenz lebendig sind. Menschen neigen dazu, Gefühle für nicht-menschliche Akteure zu entwickeln. Von Kindern, die ihre Teddybären lieben, bis hin zu Teenagern der 90er Jahre, die ihre erste digitale Beziehung zu einem Tamagotchi hatten, ist ein Trend zu beobachten, Dinge mit menschlichen Eigenschaften auszustatten. Dieses Phänomen manifestiert sich auch in der Verehrung von Statuen, Göttern und Göttinnen. Selbst bei sich bewegenden Dreiecken und Punkten neigen wir dazu, einen Willen oder eine Absicht hinter den Bewegungen zu vermuten. Probieren Sie es aus – können Sie wirklich widerstehen, hinter den Bewegungen eine Geschichte zu sehen?

Im Falle der Heider-Simmel-Illusion spielt es keine Rolle, ob wir uns dagegen sträuben, die symbolischen Bewegungen als eine Geschichte mit einer Botschaft zu interpretieren. Schliesslich kommt niemand zu Schaden, wenn man glaubt, dass das Dreieck den Punkt verfolgt. Bei den so genannten KI-Freunden, oder einfach M3gan, die dem Mädchen einen Freund ersetzen sollen, steht allerdings viel mehr auf dem Spiel. KI-Begleiter sind digitale, synthetische Wesen, die (meist) auf KI-Technologie basieren und menschliche Gesellschaft und Interaktion bieten sollen. Sie können in Form von Chatbots, virtuellen Assistenten, interaktivem Spielzeug oder humanoiden Robotern existieren und sollen dem Nutzer emotionale oder praktische Begleitung bieten. Im Gegensatz zur Heider-Simmel-Illusion kann man davon ausgehen, dass die Suche nach Gesellschaft den Menschen in einen emotional verletzlichen Zustand versetzt. Daher sind die Folgen für sie viel schwerwiegender, wenn sie das Verhalten des KI-Begleiters falsch interpretieren oder wenn sie sich zu sehr an ihn binden.

Wenn es um das Roboter-Mädchen M3gan geht, kann das erste Zusammentreffen mit unterschiedlichen Reaktionen einhergehen: Freude? Faszination? Angst? Neugier? Oft entsteht eine gewisse Disharmonie in den Gedanken der Menschen. Verwirrung entsteht, wenn der Roboter so realistisch wirkt und automatisch stellen Menschen die Frage: Was ist Mensch, was Maschine und wo unterscheiden wir uns noch? Unser Gehirn ist verwirrt, wenn es eine Maschine nicht mehr richtig als Maschine einordnen kann. Dies ist auf unsere herausragende kognitive Fähigkeit, das Anthropomorphisieren, zurückzuführen, denn unser Gehirn neigt dazu, nichtmenschliche Dinge als menschlich wahrzunehmen, um die Welt besser zu verstehen oder andere Bedürfnisse zu befriedigen. Dabei spielt Einsamkeit und/oder Isolation eine besonders grosse Rolle.

Die Diskussionen in den Medien konzentrieren sich oft auf das Design des Roboters M3gan (gespielt von einem echten Kind), aber es gibt einen Moment im Film, der auf etwas anderes hinweist: Der Moment, in dem das Mädchen seiner Tante eine Ohrfeige gibt oder panisch auf sie einschimpft, weil sie ihr den Roboter wegnehmen will. Zugegebenermassen, ein trotziges Kind würde das gegebenenfalls auch machen, wenn man ihm irgendein Spielzeug wegnimmt. Das hat v.a. bei Kleinkindern auch andere Ursachen. Aber was der Film auch hier wieder auf-

zeigt ist ein reales Problem, maskiert hinter einem hübschen Gesicht mit grossen, strahlenden Augen: Menschen bauen zu Agenten eine Mensch-KI-Beziehung auf, mit ähnlichen Beziehungs-Mechanismen, die auch bei der menschlichen Interaktion zu finden sind. Zwar kann ein bewusstes soziales Design im besten Fall die Nutzerfreundlichkeit und Spass fördern, jedoch kommt immer mehr zum Vorschein, dass es auch negative psychologische Konsequenzen für den Nutzer haben kann.

Es gibt Menschen, die mit ihren AI Chatbots, wie z.B. Xiaoice von Microsoft, so eine starke emotional Bindung aufbauen, dass sie darunter leiden, wenn die Verbindung in die Brüche geht, bis hin zu Depressionen. Oder sie werden süchtig und vergessen, wie das normale Leben aussieht und wie wir mit echten Menschen und Beziehungen umgehen, die auch Konflikte beinhalten und nicht 24/7 erreichbar sind. Es ist auch plausibel, dass so eine enge Verbindung mit einem Chatbot negative Auswirkungen auf das Sozialverhalten im echten Leben hat. Die Datenlage reicht nicht, um abschliessend eine klare Aussage zu treffen, aber erste Studien weisen neben Zeitungsberichten auf die Problemlage hin. Im schlimmsten Fall können diese Beziehungsmechanismen ausgenutzt werden, um Nutzer dazu zu verleiten, mehr Geld zu investieren, mehr Daten zu teilen und länger zu bleiben. Dies kann durch gezieltes Design erreicht werden, um das Bedürfnis des Nutzers nach Interaktion und Bindung auszunutzen. In diesem Kontext bezeichnen wir diese Praxis als Relationship Exploit.

FAZIT

M3gan hat als Film einen mässigen Unterhaltungswert, und auch wer es als Grundlage einer ethischen Auseinandersetzung nutzen will, muss tief schürfen. Aufgrund der Effekte und Ungereimtheiten in der Logik, gehen diese tieferliegenden Probleme irgendwie unter. Es wird viel zu viel diskutiert, ob es machbar wäre, so einen Roboter zu bauen und ob oder wann KI ein Bewusstsein entwickelt. Ein Problem, dass wir von den Diskussionen mit AGI Believern kennen. AGI Believer sind Menschen, die davon überzeugt sind, dass es möglich ist, künstliche Intelligenz zu schaffen, die genauso fortschrittlich und mächtig ist wie die menschliche Intelligenz. Sie glauben an die Möglichkeit einer künstlichen Allgemeinen Intelligenz (AGI), die in der Lage ist, eine Vielzahl von Aufgaben zu lösen und Entscheidungen zu treffen, ähnlich wie ein menschliches Gehirn. Diese

im wahrsten Sinne des Wortes fantastischen Fragestellungen und Diskussionen, lenken wie so oft ab von den realen Problem, die mit der Einführung neuer Technologien und deren oft unreflektierter Vermarktung einhergehen. Diese Ablenkung von den realen Problemen hat jedoch Konsequenzen. Es besteht die Gefahr, dass wichtige Themen und potenzielle Risiken unbeachtet bleiben, wie z.B. Datenschutz, ethische Fragen und die Auswirkungen auf die Gesellschaft. Daher ist es von grösster Bedeutung, dass wir uns mit diesen Themen kontinuierlich auseinandersetzen und einen kritischen Diskurs führen, Hype und Hirngespinste entlarven, um sicherzustellen, dass wir die Technologie für unser Wohl nutzen, anstatt uns von ihr – und deren Herren der Schöpfung – ausnutzen zu lassen.

Marisa Tschopp

next gen vulnerability intelligence

VulDB

Vulnerability Management mit Splunk

Laden Sie einfach und unkompliziert die Daten für das Vulnerability Management Ihrer Umgebung in Splunk. Die frei installierbare Applikation nutzt die offene API von VulDB, um Daten einzulesen, abzulegen und aufzuarbeiten. Noch nie war Vulnerability Management so einfach. Setzen Sie sich mit uns in Verbindung!

)SCIP(
official data provider

> https://vuldb.com

ANDREA HAUSER

PROTOTYPE POLLUTION ALS JAVASCRIPT-ANGRIFFSTECHNIK

Bei JavaScript Prototype Pollution handelt es sich um eine JavaScript-Schwachstelle, mit der Properties zum globalen Prototype hinzugefügt werden können; keine Angst, wenn Ihnen dies nichts sagt, im Artikel werden auf die notwendigen JavaScript Grundlagen eingegangen. Diese Schwachstelle kann client-seitig für Cross-Site-Scripting und server-seitig im schlimmsten Fall für Remote-Code-Execution ausgenutzt werden.

Dieser Abschnitt beschreibt JavaScript-Grundlagen, wenn Sie sich mit JavaScript bereits auskennen, können Sie diesen Abschnitt problemlos überspringen.

WAS IST EIN OBJEKT IN JAVASCRIPT?

Ein Objekt ist eigentlich nur eine Ansammlung von Properties, wobei Properties key:value Paare sind. Ein Objekt sieht wie folgt aus:

```
var exampleObject = {
    test: "value",
    exampelMethod: function() {
        //do something here
        console.log("test")
    }
}
```

Auf die Properties eines Objekts können wie folgt zugegriffen werden:

```
exampleObject.test
```

oder

```
exampleObject['test']
```

und die Methode eines Objekts kann wie folgt aufgerufen werden:

```
exampleObject.exampleMethod();
```

Beim Beispiel oben handelt es sich um ein explizit deklariertes Objekt, in JavaScript basiert allerdings fast alles im Hintergrund auf Objekten. Gelöst wird das ganze über den Prototype.

WAS IST DER JAVASCRIPT PROTOTYPE?

Beim Prototype handelt es sich um den Mechanismus, mit dem in JavaScript Elemente von Objekten an andere Objekte vererbt werden. Der Prototyp eines Objekts ist nichts anderes als ein weiteres Objekt, das ebenfalls einen eigenen Prototyp hat. Und da praktisch alles in JavaScript unter der Oberfläche ein Objekt ist, führt diese Kette letztlich zum obers-

ten Object.prototype zurück, dessen Prototyp dann einfach der Wert null ist.

In der Praxis bedeutet das, dass JavaScript im Hintergrund folgendes macht, wenn auf ein Property mittels exampleObject.test oder exampleObject['test'] zugegriffen wird:

1. Die JavaScript-Engine sucht nach dem Property test in dem Objekt exampleObject.

2. Falls das Property vorhanden ist, wird es zurückgegeben. Ansonsten wird der Prototype des benutzerdefinierten Objekts genommen und in diesem nach dem Property gesucht. Diese Suche wird in der Prototype-Kette so lange fortgeführt, bis das Property gefunden wurde, oder bei obersten, also dem null, Prototype angelangt wird und dort wird dann undefined zurückgegeben.

Auf einem Objekt kann wie folgt auf den Prototype zugegriffen werden:

- __proto__

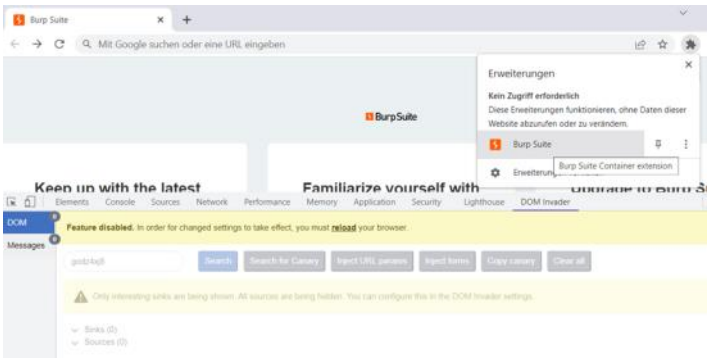
- constructor.prototype

Mit diesen Grundlagen sollten Sie nun in der Lage sein, JavaScript Prototype Pollution zu verstehen.

PROTOTYPE POLLUTION

Bei einer Prototype Pollution hat ein Angreifer das Ziel Object.prototype zu verändern. Da beinahe alle Elemente in JavaScript von Objekt erben, können damit beinahe alle Elemente angegriffen werden. In den meisten Fällen wird Prototype Pollution durch eine unsicher merge Funktion ausgelöst, die rekursiv Properties aus einer nicht vertrauenswürdigen Quelle übernimmt. Olivier Arteau beschreibt eine solche merge Funktion in seinem Paper Prototype pollution attack in NodeJS application wie folgt:

```
merge(target, source)
    foreach property of source
        if property exists and is an object
on both the target and the source
```




```
            merge(target[property], source
[property])
        else
            target[property] = source
[property]
```

Für Prototype Pollution wird folgendes benötigt:

Source, also der Ort, an dem die Pollution übergeben werden kann

- URL
- JSON
- Web Message
- Die Suche dafür ist manuell sehr aufwendig, vor allem wenn der JavaScript-Code minified wurde. Es wird empfohlen Tools wie den DOM Invader in Burp zu verwenden.

Sink

- Für DOM-XSS, eine JavaScript-Funktion oder ein DOM-Element, das JavaScript Code Ausführung erlaubt

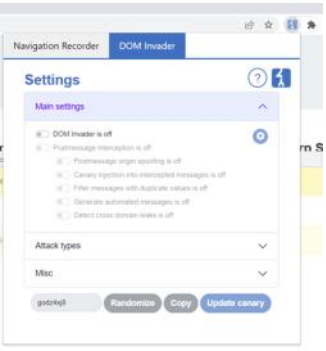
Gadget, ein Property, dass ohne Bereinigung an die Sink weitergegeben wird

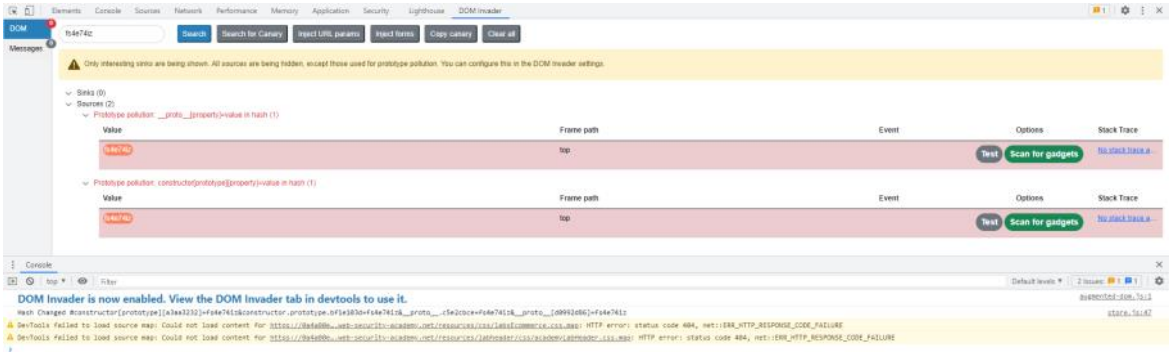
- Also das Element das Source und Sink verbindet

Auffinden von Prototype Pollution mit Burp DOM Invader

Beim DOM Invader handelt es sich um eine Erweiterung des im Burp mitgelieferten Chromium Browsers. Diese Erweiterung ist im Normalfall deaktiviert, da sie ungewünschte Nebenwirkungen haben kann.

Im Burp mitgelieferten Browser die Erweiterung mit dem Titel Burp Suite auswählen.





Und in dem sich öffnenden Fenster DOM Invader auswählen und aktivieren.

Sobald die Erweiterung aktiv ist, kann die Webseite, die auf Prototype Pollution untersucht werden soll, neu geladen werden. Damit wird der DOM Invader im Hintergrund richtig aufgesetzt. In den Developer Tools gibt es nun einen neuen Eintrag mit dem Titel DOM Invader. Wenn dieser Ausgewählt wird, werden die Resultate der Analyse des DOM Invaders angezeigt. Im untenstehenden Beispiel wurden zwei Prototype Pollution Möglichkeiten identifiziert.

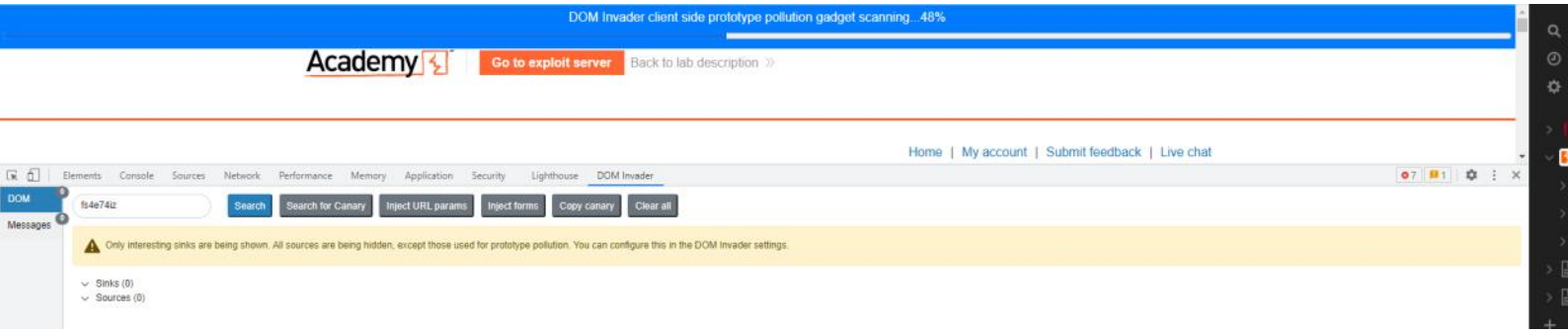
Im einfachsten Fall kann einfach die Option Exploit ausgewählt werden und es wird ein alert(1) ausgeführt. Falls kein alert auftaucht sollte in der Konsole die Fehlermeldung anzeigt werden und mittels dem dort vorhandenen StackTrace landet man im JavaScript an dem Ort, an dem die Prototype Pollution schiefläuft. Von da kann man dann einfach die Payload analysieren und wie erwartet anpassen, so dass der alert ausgeführt wird.

Auffinden von Prototype Pollution von Hand

Die manuelle Suche nach JavaScript Prototype Pollution kann sehr aufwendig sein, vor allem dann, wenn der von der Webseite genutzte JavaScript Code minified wurde. Wie dafür vorgegangen werden kann, wurde in den Artikeln von Portswigger und Nikita Stupin besser und tiefergehend eingegangen, als dass es hier gemacht werden kann. Die Lektüre dieser Artikel ist sehr empfehlenswert, um das Wissen zu Prototype Pollution zu vertiefen. Insbesondere der Portswigger-Artikel ist empfehlenswert, da dort auch Labs angeboten werden, bei denen die gelernten Techniken direkt angewendet werden können.

GEGENMASSNAHMEN

Es gibt unterschiedliche Möglichkeiten, wie man sich gegen JavaScript Prototype Pollution schützen kann. Diese kommen jeweils mit unterschiedlichen Vor- und Nachteilen:



Object mit Object.create(null) erstellen

- Das so definierte Objekt hat keinen Prototype und erbt damit auch nicht von JavaScript Object
- Problematisch ist, dass damit Standardfunktionen wie toString()nicht mehr verwendet werden können, da diese Standardfunktionen über das Object Prototype an benutzerdefinierte Objekte vererbt werden.

Deny-List mit Begriffen wie zum Beispiel __proto__

- Deny-Lists sind grundsätzlich meist eine schlechte Idee, da solche Listen oft durch das Verwenden einer anderen Syntax umgangen werden können.

Object.freeze() verwenden

- Damit kann Object Prototype nicht mehr verändert werden
- Dies kann allerdings zu unerwarteten Problemen führen, wenn Abhängigkeiten den Object Prototype dennoch verändern möchten; alternativ kann Object.seal() verwendet werden, dann können keine neuen Properties mehr definiert werden, aber bestehende Properties können noch verändert werden.

Da ein Angriffsweg via JSON ist, sollte das von Benutzern oder aus anderen unsicheren Quellen erhaltene JSON gegenüber einem vordefinierten JSON-Schema geprüft werden und alle Parameter, die nicht im Schema definiert sind, sollten verworfen werden.

ZUSAMMENFASSUNG

Bei JavaScript Prototype Pollution handelt es sich um eine komplexe Angriffsmöglichkeit, die in den schlimmsten Fällen zu XSS oder server-seitig sogar zu RCE führen können. Das Auffinden solcher Schwachstellen ist zwar manuell möglich, ist allerdings sehr aufwändig, da die meisten modernen Webseiten viel und meist minified JavaScript Code haben. Da Portswigger, die Hersteller von Burp, sich ausgiebig mit dem Thema beschäftigt haben, wird innerhalb von Burp allerdings gutes Tooling zur Identifizierung dieses Schwachstellen-Typs zur Verfügung gestellt. Für Entwickler bestehen unterschiedlichste Möglichkeiten mit verschiedenen Vor- und Nachteilen, um JavaScript-Code gegen Prototype Pollution zu härten.

Andrea Hauser

ROBUSTHEIT KANN UND SOLLTE STETS AUCH SIMPEL SEIN

Bildquelle: https://pixabay.com/images/id-3770499/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch