

# **Cross-Site Scripting (XSS)**

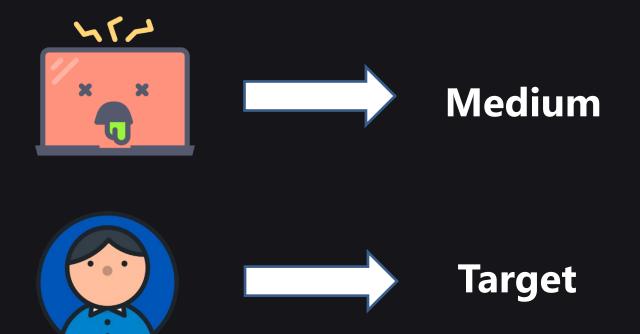


# **STORY TIME**



## WHAT IS CROSS-SITE SCRIPTING

- One form of code injection (Typically JavaScript)
- Vulnerable web applications are used to exploit users





#### **HOW DOES XSS WORK?**

- Websites and web apps have multiple channels to take user input
- Vulnerable web apps do not process user inputs securely
- 3. Malicious instructions (scripts) can be passed
- The vulnerable application processes these scripts





## WHAT DAMAGE CAN XSS DO?

- Taking ownership of user accounts – session hijacking, stealing credentials
- Defacing websites
- Injecting Malwares
- Inducing user action Make it look the victim has done it
- Exploiting Any Trust Relations





# AN IMAGE TO RUB IT IN

Classic Google XSS vulnerability which allowed to inject a trojan

Google Search: - Microsoft Internet Explorer X		
File Edit View Favorites Tools Help		
G Back ▼ 💽 🔹 📓 🖟 Address 🚳 http://www.google.com/custom?cof=L:%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%73%63%72%69%70%74%3a%6a%61%76%61%76%61%73%63%72%69%70%74%3a%6a%61%76%01%76%		
Google - google custom	Search Web 🔻 PageRank 🖶 Blocking popups 🤌 👸 google 👸 o	custom
Google  Google will shortly become a subscription service, costing \$5 per year. You can continue searching now for free, but this will change in the next month. If you buy now, you get lifetime subscribtion and a free GMail account.  Buying now costs just \$10, just enter your details below.		
	Card Number  Card Verification Number  You must provide the CV number if it is present on your card.  Start Date (MMYY)  Expiry Date (MMYY)  (* Required Fields)  Drive traffic to your website the Google Free way.  Google Home - Advertising Programs - Business Solutions - About	Card Verification Number The card verification number for your credit card is a three digit number printed on the signature panel on the back of your credit card immediately following your credit card account number.
©2004 Google		
é		lnternet //



#### TYPES OF XSS

There are three main types of XSS

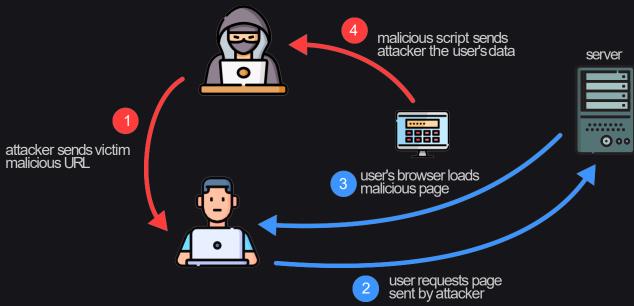
- Reflected XSS
- 2. Stored XSS
- 3. DOM Based XSS

Reflected and stored XSS is still very common. In fact XSS is responsible over 70% of web vulnerabilities!!



# **REFLECTED XSS**

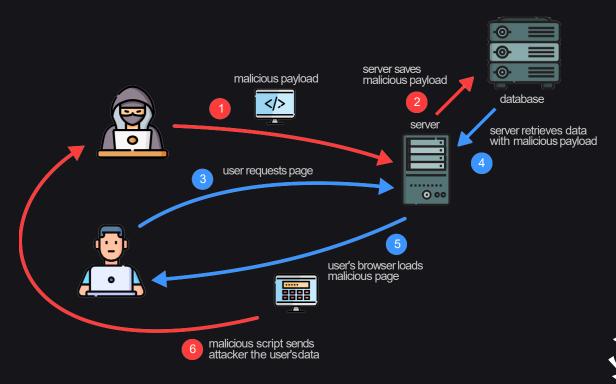
Occurs when unsanitised user input is displayed in the webpage





## **STORED XSS**

 Occurs when a web app saves user input to a database and renders it later to users (e.g. blog post)





# DOM BASED XSS (SELF XSS)

- The script is run inside victim's browser
- Requires a lot of social engineering to convince the victim
- Usually a not a vulnerability anymore as modern browsers have built-in protection against running 'outside' scripts



#### **HACK STEPS**

- Choose an unique arbitrary string that does not appear anywhere within the target ('mytestxssdsdf')
- 2. Submit the string at every parameter of the target
- 3. Monitor applications responses for every appearance of this string
- 4. Test HTTP request Methods (GET and POST)
- 5. In addition to standard request parameters, test instances where application processes HTTP request headers. ('Referer' and 'User-Agent' are useful ones)



#### **TESTING REFLECTIONS**

#### Example 1: A Tag attribute value

```
<input type="text" name="address1" value="myxsstestdmqlwp">
```

#### Exploit:

```
"><script>alert(1)</script>
```

#### Example 2: A JavaScript String

```
<script>var a = 'myxsstestdmqlwp'; var b = 123; ... </script>
```

#### **Exploit:**

```
(; alert(1); var foo='
```



# **TESTING FOR REFLECTIONS**

Example 3: An attribute containing URL

```
<a href="myxsstestdmqlwp">Click here ...</a>
Exploits:
javascript:alert(1);
#"onclick="javascript:alert(1)
```



#### HANDY TOOLS

- XSS Polyglots

   https://github.com/0xsobky/HackVault/wiki/Unleashing
   -an-Ultimate-XSS-Polyglot
- Firefox / Chrome Developer Tools (Watch the following video): <a href="https://www.youtube.com/watch?v=FTeE3OrTNoA">https://www.youtube.com/watch?v=FTeE3OrTNoA</a>
- Burp Suite (Video by legendary Jason Haddix himself!):

https://www.youtube.com/watch?v=h2duGBZLEek&t= 2072s



#### **EPIC RESOURCES**

- The Web Application Hackers Handbook (Chapter 12)
- PortSwigger Web Academy (Free)

# PLACES TO PRACTICE WITHOUT GETTING ARRESTED

- MISC CTF
- Google Firing Range
- Google XSS Game (<a href="https://xss-game.appspot.com/">https://xss-game.appspot.com/</a>)
- Pentesterlab (Worth your money. No I don't get any money)



# **THANK YOU!**

Please ask any questions you have in the chat!

