CsFire: Browser-Enforced Mitigation Against CSRF

Lieven Desmet and Philippe De Ryck
DistriNet Research Group
Katholieke Universiteit Leuven, BE

Lieven.Desmet@cs.kuleuven.be

OWASP
23/06/2010

The OWASP Foundation
http://www.owasp.org

About myself

- Lieven Desmet

- Research manager of the DistriNet Research Group (K.U.Leuven, Belgium)

- Active participation in OWASP:
  - Board member of the OWASP Belgium Chapter
  - Co-organizer of the academic track on past OWASP AppSec Europe Conferences

Outline

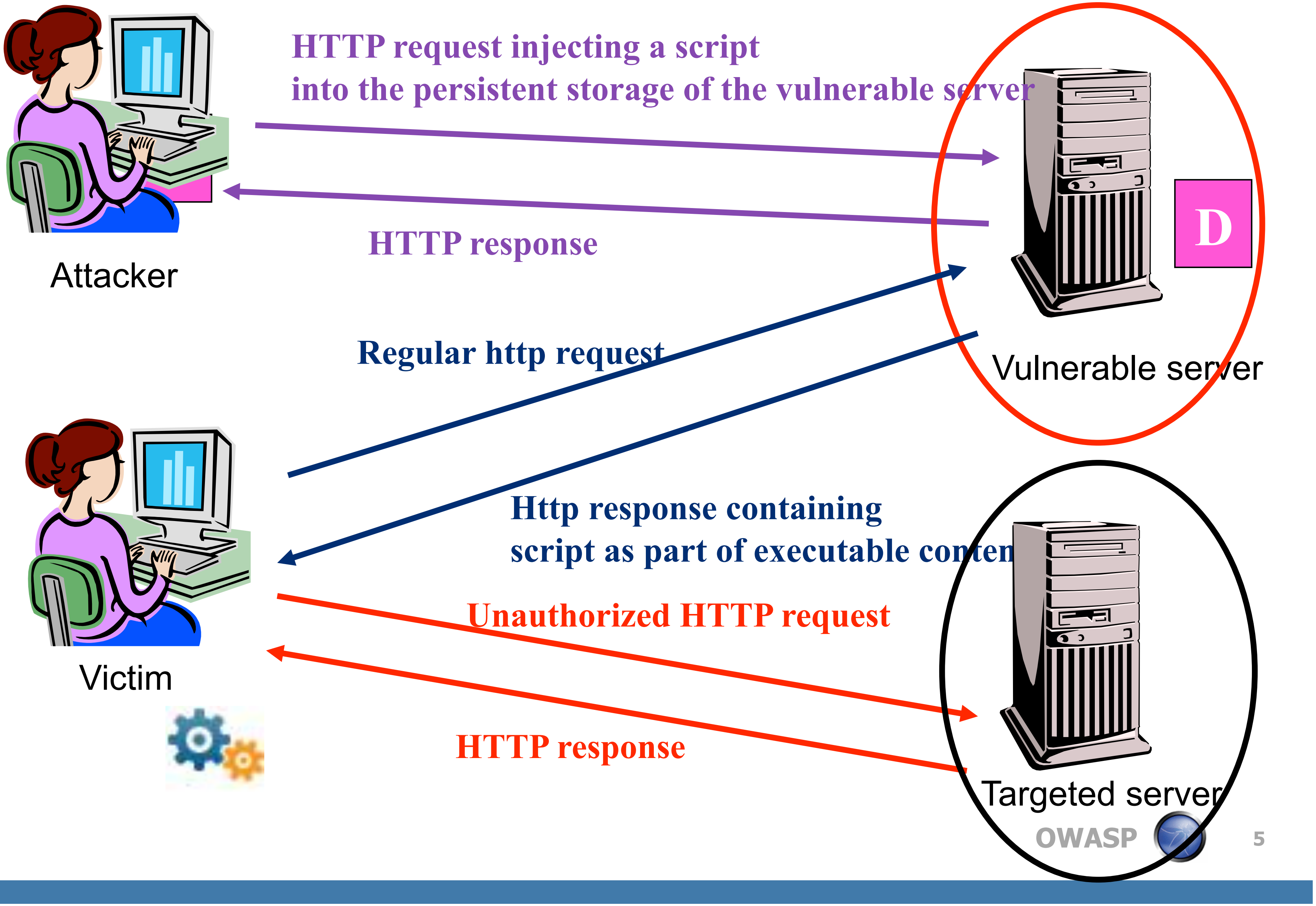
- Introduction
- Quantification of cross-domain traffic
- Client-side mitigation against CSRF
- CsFire
- Evaluation
- Conclusion

Cross-Site Request Forgery (CSRF)

- Synonyms: one click attack, session riding, confused deputy, XSRF, …

- Description:
  - External server (or HTML feed) is under control of the attacker
  - Attacker triggers requests from the victim’s browser to targeted website:
    - Unauthorised by the victim
    - Legitimate from the perspective of the server
  - Victim typically has an account of the targeted server (and is logged in)

CSRF (+XSS) example


HTTP request injecting a script
into the persistent storage of the vulnerable server
HTTP response
Attacker
D
Vulnerable server
Regular http request
Http response containing
script as part of executable content
Unauthorized HTTP request
HTTP response
Victim
Targeted server

Implicit authentication

- HTTP authentication: basic, digest, NTLM, …
- Cookies containing session identifiers
- Client-side SSL authentication
- IP-address based authentication
- …

- Notice that some mechanisms are even completely transparent to the end user!
  - NTLM, IP-address based, …

Risk considerations

- Threat agent:
  - Any website or HTML feed that your users access
- Impact:
  - Sending unauthorized requests
  - Login CSRF
  - Attacking the Intranet

[BJM08]

CSRF in practice

- W. Zeller and W. Felten, Cross-site Request Forgeries: Exploitation and Prevention, Technical Report 2008

[ZF08]

- CSRF in the ‘real’ world
  - New York Times (nytimes.com)
  - ING Direct (ingdirect.com)
  - Metafilter (metafilter.com)
  - YouTube (youtube.com)

Outline

- Introduction
- Quantification of cross-domain traffic
- Client-side mitigation against CSRF
- CsFire
- Evaluation
- Conclusion

Quantification of cross-domain traffic

- Need for better insights
  - To identify the nature of nowadays web interactions
  - To find an appropriate balance between usability and security
- Analysis of real-life traffic
  - 50 grad students
  - 10 week period
  - Total: 4.7M requests

Data collection

- Via custom-made browser extension
  - Fully transparent for the end-user
  - Extension installed as part of lab exercise

- Logs relevant information for each outgoing request
  - Originator:
    - Domain, scheme, DOM element, …
  - Request:
    - Target domain, scheme, method, URL path, input parameter keys, cookie keys, HTTP auth?, user interaction?, redirect?, …

Privacy considerations

- Only keys were recorded, no values or credentials
  - Cookies
  - Input parameters
  - HTTP authentication
- Full URLs were not recorded
  - Only filename + extension
- No client information was recorded
  - No browser information (except for logger version)
  - No IP information
  - No usernames

Quantification of cross-domain requests

	GET	POST	Total
cross-domain requests (strict SOP)	1,985,052 (41.97%)	59,415 (1.26%)	2,044,756 (43.24%)
cross-domain requests (relaxed SOP)	1,503,990 (31.80%)	56,260 (1.19%)	1,560,519 (33.00%)
All requests	4,426,826 (93.61%)	302,041 (6.39%)	4,729,217 (100.00%)

Cross-domain requests characteristics (under relaxed SOP)

	Input parameters	User initiated	Cookies	HTTP auth	Total
GET requests	533,612 (35.47%)	6,837 (0.45%)	528,940 (35.17%)	1,357 (0.11%)	1,503,990
POST requests	41 (0.07%)	26,914 (47.84%)	12,442 (24.36%)	269 (0.01%)	1,560,519

Interesting conclusions

- Large number of requests has
  - Input parameters (+-35%)
  - Cookies (+-35%)
- Use of HTTP authentication is very limited

- Additional information:
  - Total number of requests: 4,729,217
  - Total number of domains: 23,592
    - 3338 domains use redirects (14.15%)
    - 5606 domains use cookies(23.76%)
    - Only 2 domains use HTTP authentication

Need for more benchmarks and data sets

- Interesting data set to study and compare CSRF mitigation techniques

- It would be interesting to have more similar data sets available for web application security
  - To understand nature of nowadays web applications and interactions
  - To have benchmarks to compare different solutions

Outline

- Introduction
- Quantification of cross-domain traffic
- Client-side mitigation against CSRF
- CsFire
- Evaluation
- Conclusion

Mitigation against CSRF

- Same-Origin Policy
  - No protection against CSRF ☹
  - Enabler for token-based approaches

- Token-based approaches
  - Most promising techniques against CSRF ☺
  - Not widely adopted yet ☹

- Client-side mitigation !?!

RequestRodeo (Martin Johns, 2006)

- Token-based approach, run as client-side proxy
  - Intercepts requests and responses
  - Adds and verifies tokens
  - Strips cookies and HTTP authentication credentials
  - Also protects the intranet via external proxy

- Works well on classical web applications

- Behaves badly in web 2.0 applications

Browser Add-ons

- Browser add-ons can use full context
  - CSRF protector, BEAP (antiCSRF), RequestPolicy, NoScript, CsFire, …
- Mitigation: blocking or stripping request
- Hard to find right balance:
  - Security
  - Usability

Requirements for client-side mitigation

- R1. Independent of user input
  - Substantial fraction of cross-domain traffic
  - Most users don’t know necessary/safe interactions

- R2. Usable in a web 2.0 environment
  - Mashups, AJAX, Single-Sign On, …

- R3. Secure by default
  - Minimal false positives in default operation mode

Outline

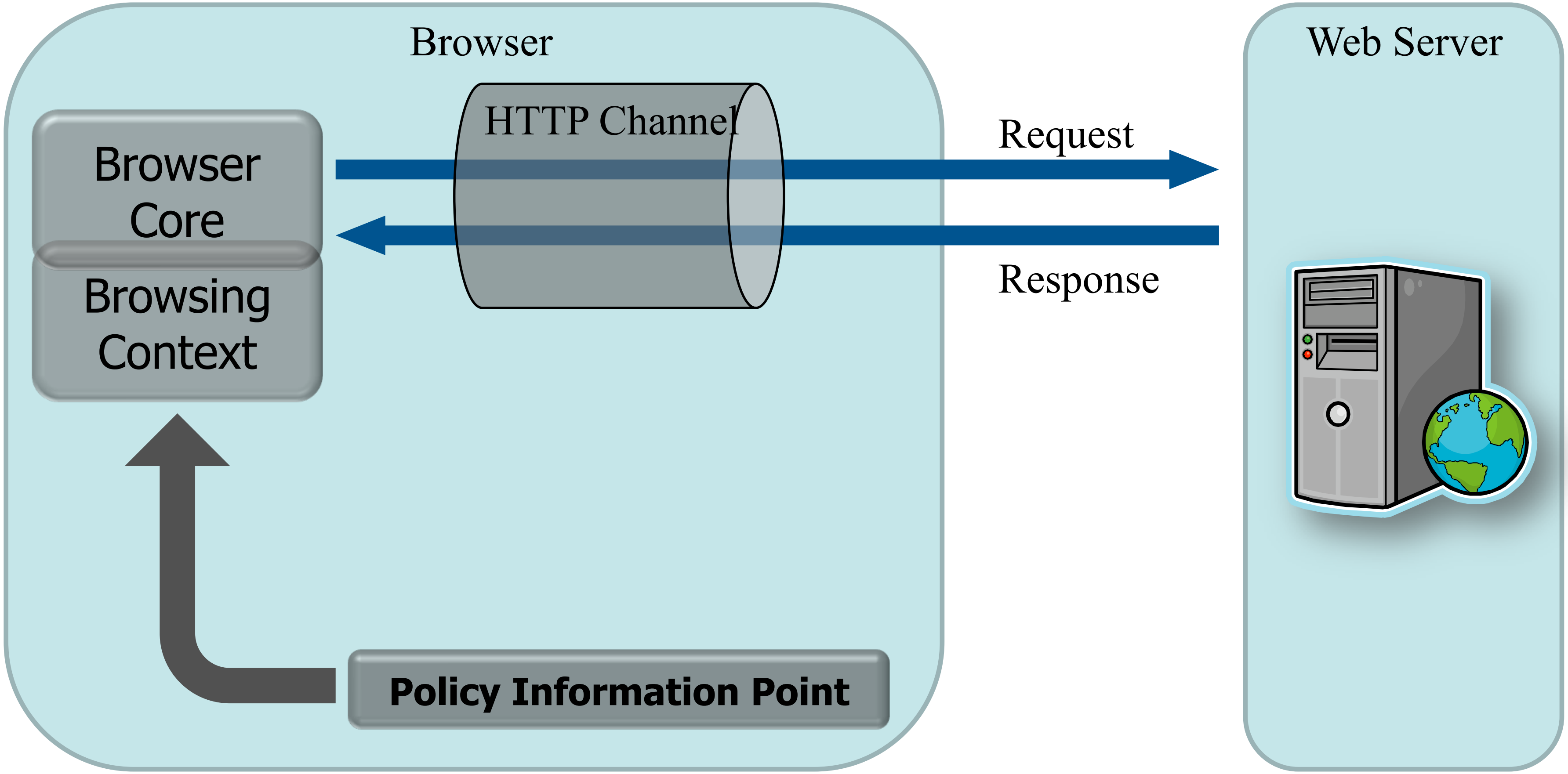
- Introduction
- Quantification of cross-domain traffic
- Client-side mitigation against CSRF
- CsFire
- Evaluation
- Conclusion

CsFire

- Client-side mitigation technique developed by DistriNet, K.U.Leuven
- Builds on RequestRodeo's concept of stripping

- Main purpose:
  - Finding a better balance between security and usability
- Full paper available:
  - Ph. De Ryck, L. Desmet, T. Heyman, F.Piessens, W. Joosen. CsFire: Transparent client-side mitigation of malicious cross-domain requests, LNCS volume 5965, pages 18-34, Pisa, Italy, 3-4 February 2010

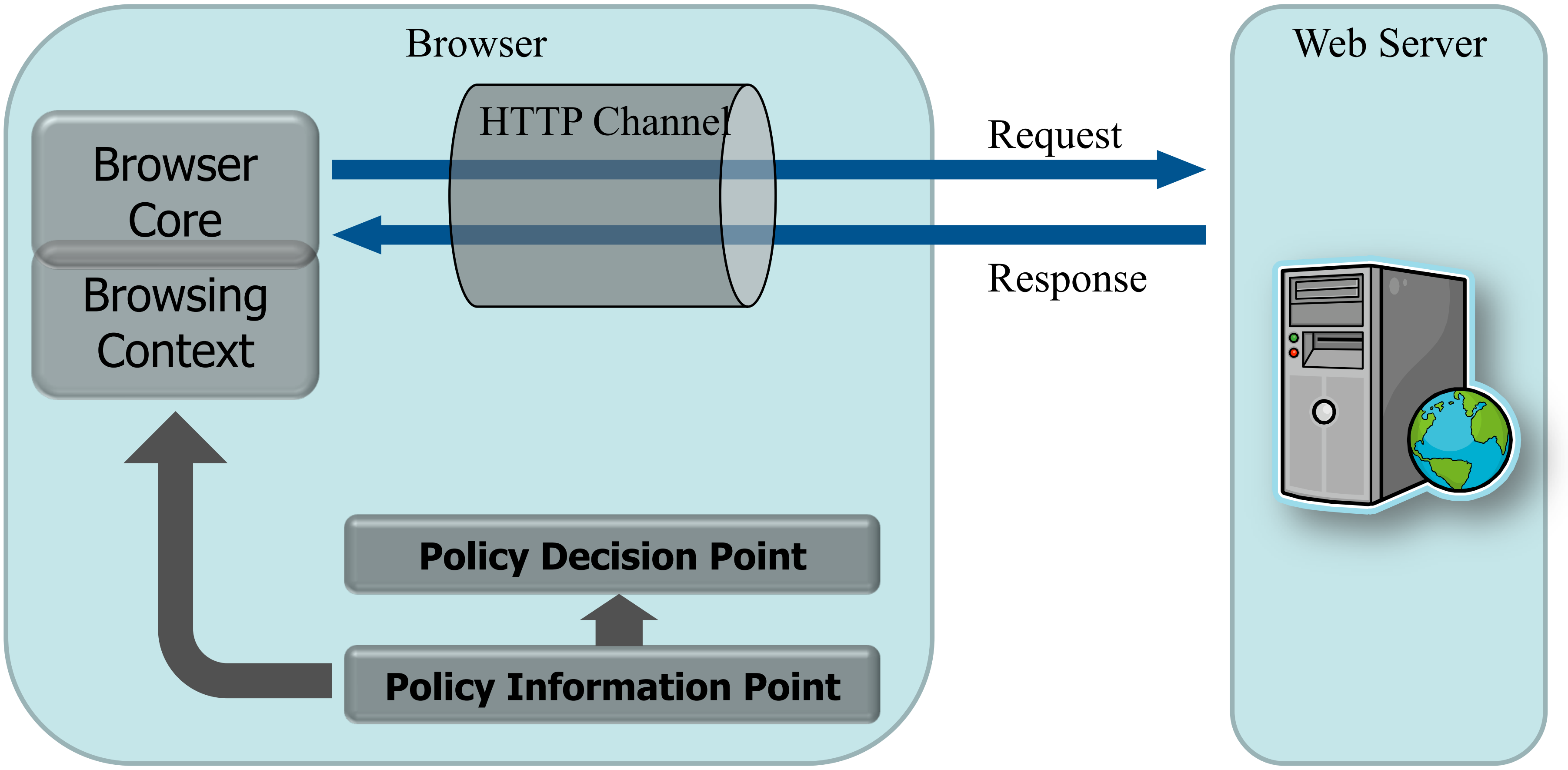
Client-side Policy Enforcement



Client-side Protection

- Collect Information
  - Origin and Destination
  - HTTP Method
  - Cookies or HTTP authentication present
  - User initiated
  - …

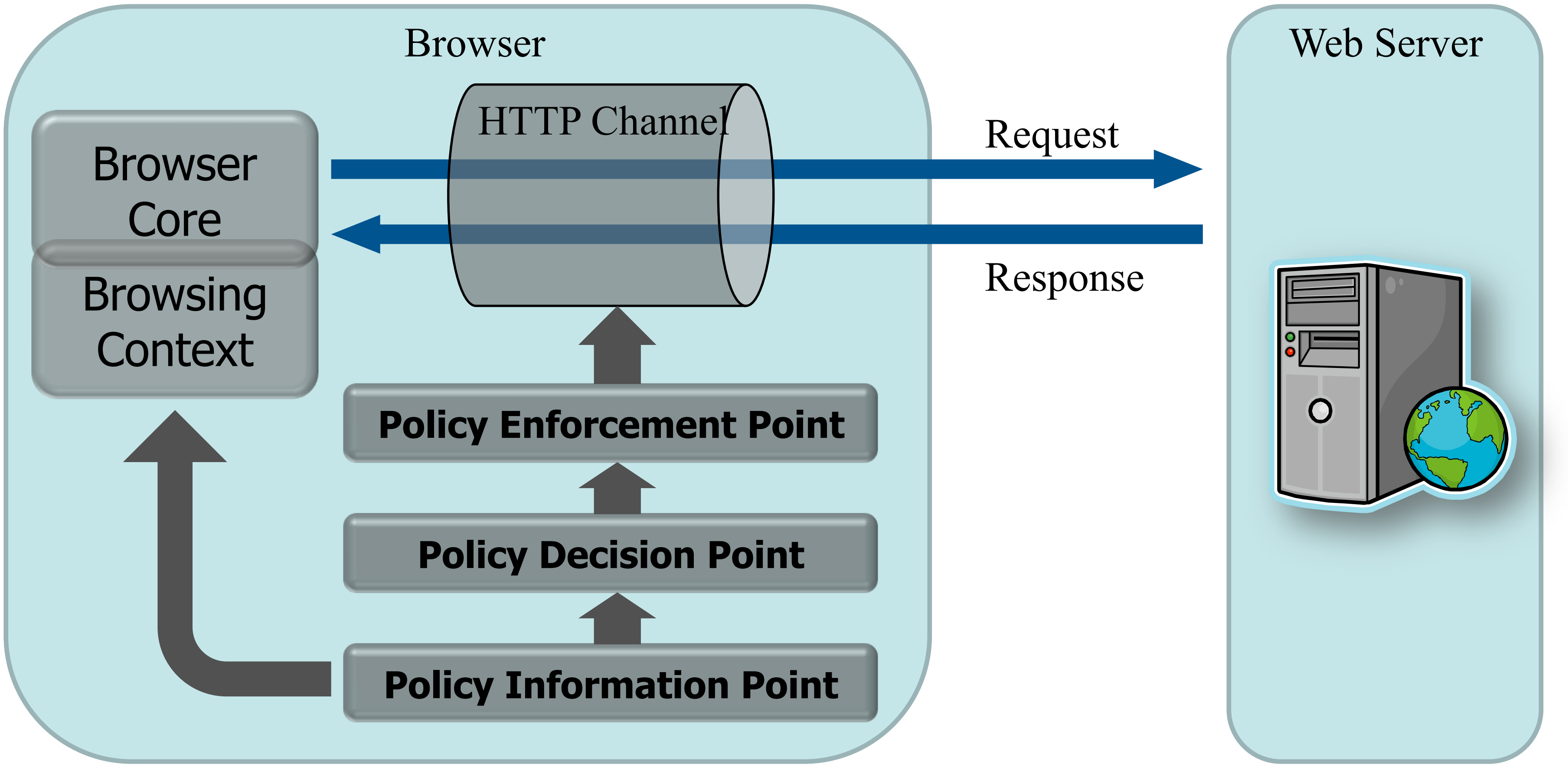
Client-side Policy Enforcement



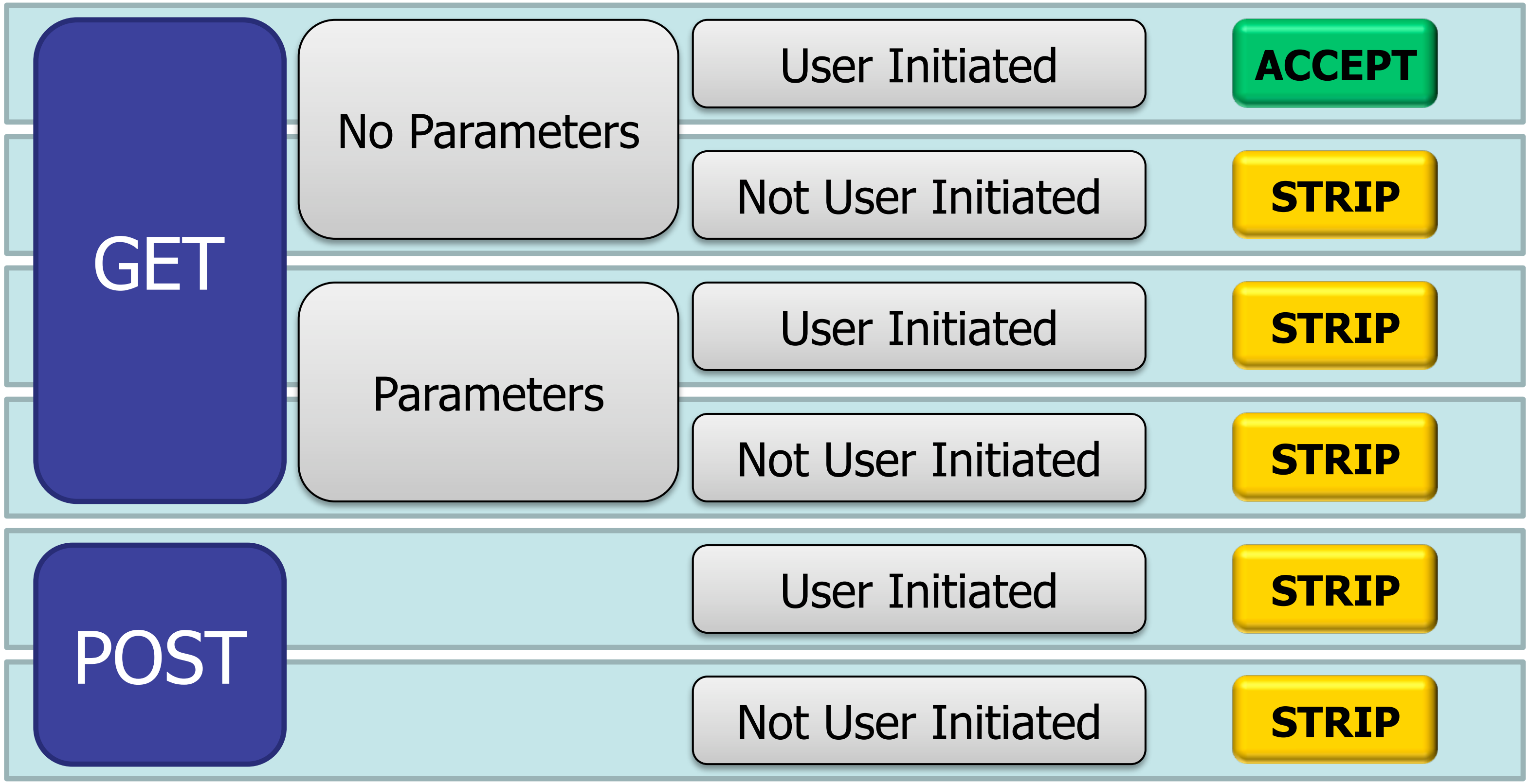
Client-side Protection

- Determine action using policy
  - Accept
  - Block
  - Strip cookies
  - Strip authentication headers

Client-side Policy Enforcement



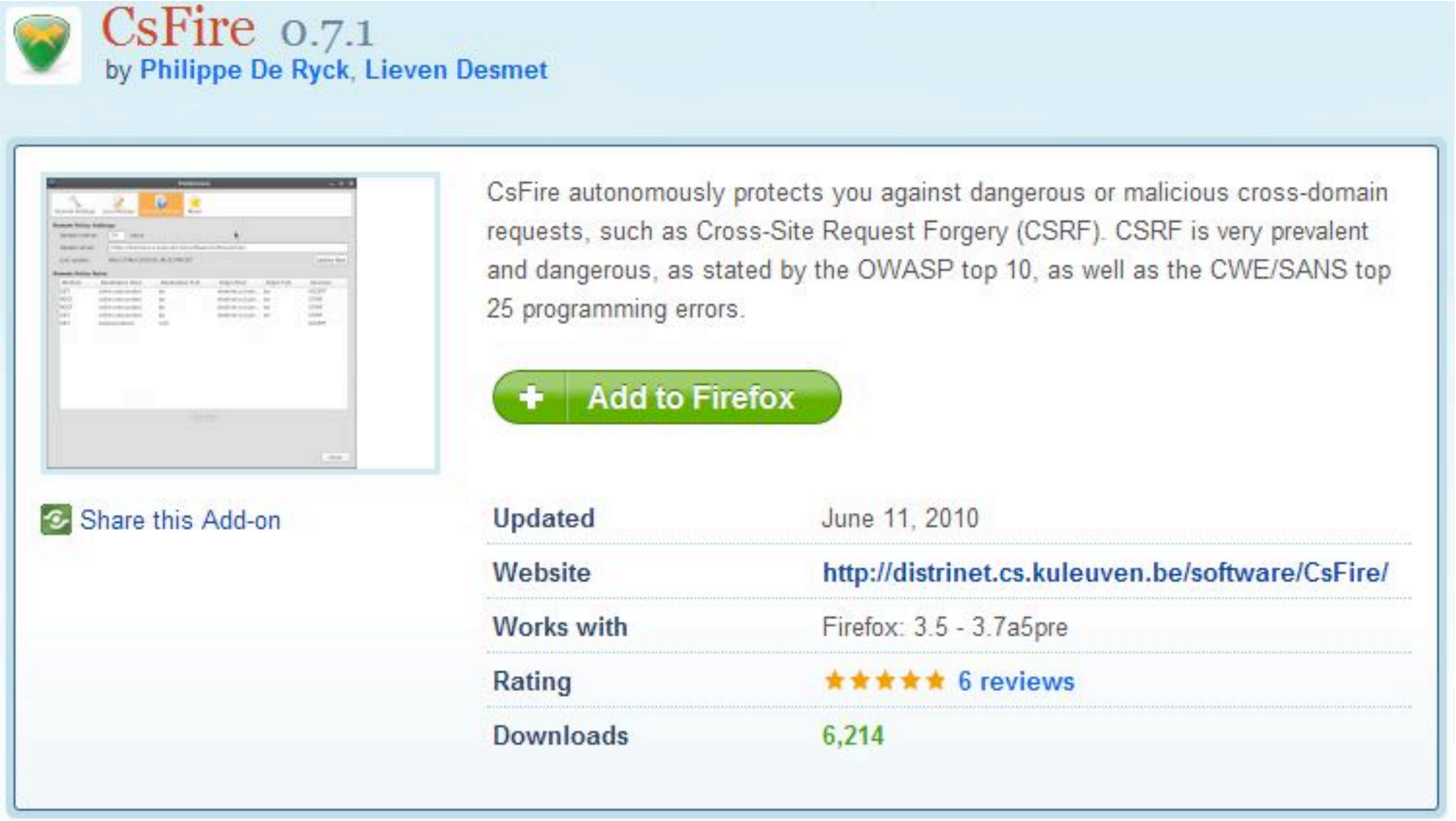
Cross-domain Client Policy



GET	No Parameters	User Initiated	ACCEPT
		Not User Initiated	STRIP
	Parameters	User Initiated	STRIP
		Not User Initiated	STRIP
POST		User Initiated	STRIP
		Not User Initiated	STRIP

Prototyped as CsFire

- http://distrinet.cs.kuleuven.be/software/CsFire



CsFire 0.7.1

by Philippe De Ryck, Lieven Desmet

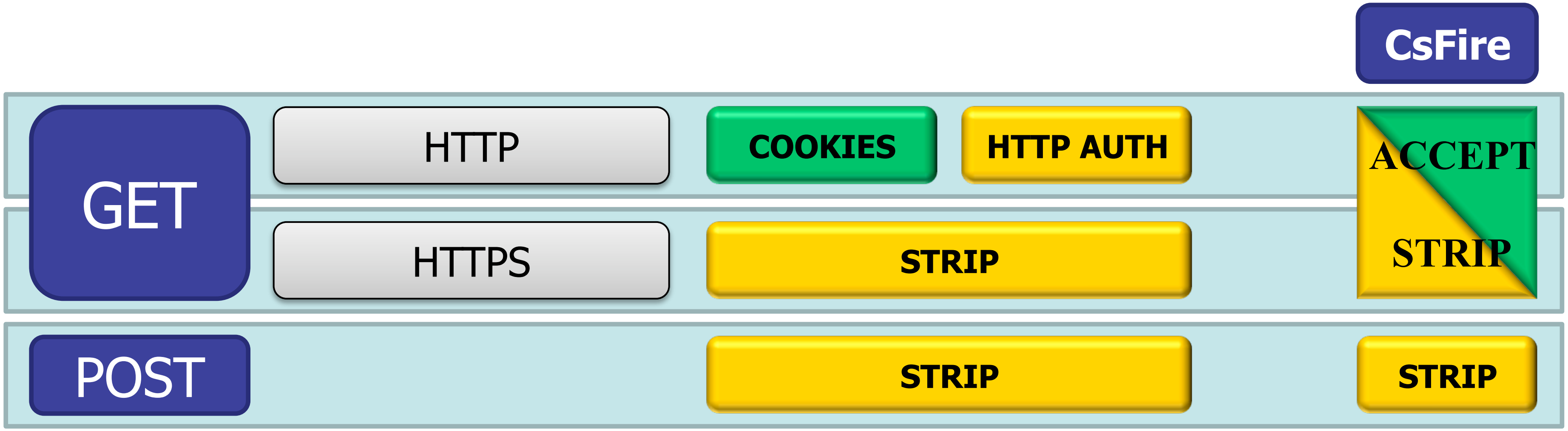
CsFire autonomously protects you against dangerous or malicious cross-domain requests, such as Cross-Site Request Forgery (CSRF). CSRF is very prevalent and dangerous, as stated by the OWASP top 10, as well as the CWE/SANS top 25 programming errors.

Updated	June 11, 2010
Website	http://distrinet.cs.kuleuven.be/software/CsFire/
Works with	Firefox: 3.5 - 3.7a5pre
Rating	★★★★★ 6 reviews
Downloads	6,214

Comparison: Request Policy

				CsFire
GET	No Parameters	User Initiated	ACCEPT	ACCEPT
		Not User Initiated	BLOCK	STRIP
	Parameters	User Initiated	ACCEPT	STRIP
		Not User Initiated	BLOCK	STRIP
POST		User Initiated	ACCEPT	STRIP
		Not User Initiated	BLOCK	STRIP

Comparison: BEAP (AntiCSRF)



				CsFire
GET	HTTP	COOKIES	HTTP AUTH	ACCEPT STRIP
	HTTPS	STRIP		
POST		STRIP		STRIP

Outline

- Introduction
- Quantification of cross-domain traffic
- Client-side mitigation against CSRF
- CsFire
- **Evaluation**
- Conclusion

Prototype Evaluation

- CSRF Scenarios
  - 59 scenarios
  - Test prevention capabilities
  - Contains attacks launched from …
    - CSS Attributes
    - HTML attributes
    - JavaScript
    - Redirects

Prototype Evaluation

- Real-life test users
  - 60 test users, several weeks
  - Detect issues in security – usability balance
  - Option to provide feedback

- Feedback via Mozilla Add-On users
  - About 6300 downloads since release
  - 1850+ daily users
    - Positive feedback
    - Some suggestions for additional server policies

Evaluation Results

- CSRF scenarios passed successfully
- Test users: very positive
  - Only a few minor inconveniences detected
    - Re-authentication after cross-domain request
  - Works well with Web 2.0
  - Works well popular SSO mechanisms

- Issues with sites spanning multiple domains
  - Example: Google, Microsoft (Live, MSN, …)

Evaluation Results

- Sites spanning multiple domains
  - Traffic resembles a CSRF attack
  - Client cannot distinguish legitimate traffic
- Additional information needed
  - Specify intended cross-domain requests
  - Server policy identifies desired cross-domain requests
- In CsFire prototype
  - Server policies via policy server
  - Local policies

Outline

- Introduction
- Quantification of cross-domain traffic
- Client-side mitigation against CSRF
- CsFire
- Evaluation
- Conclusion

Conclusion

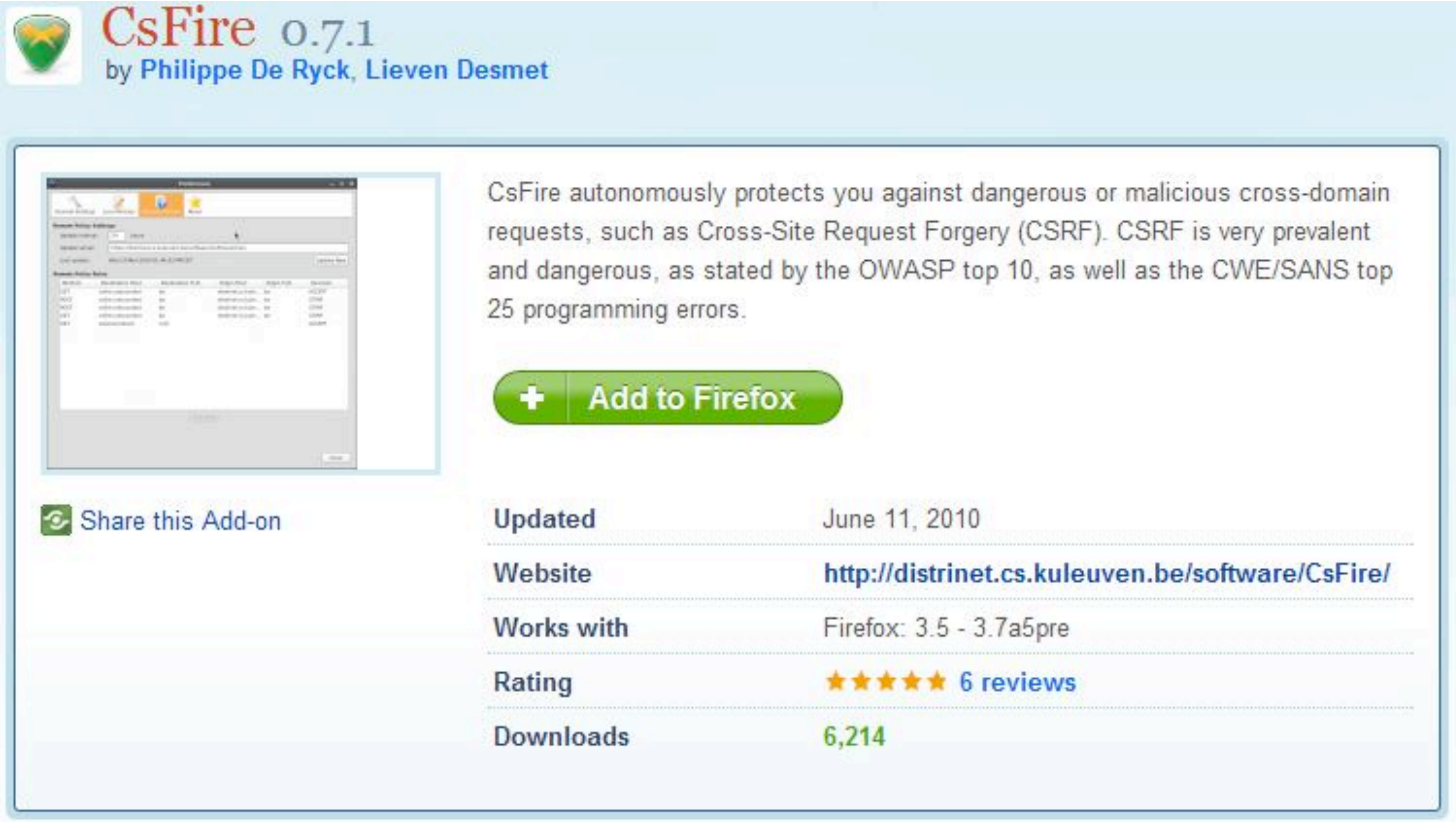
- Traffic analysis reveals cross-domain traffic patterns
- Requirements for a client-side solution
  - Security
  - Usability
- Balanced client-side solution
  - Secure by default
  - User-independent
- Implementation as Firefox add-on
  - Technical evaluation with CSRF scenarios
  - Real-life evaluation with test users

References

- W. Zeller and W. Felten, Cross-site Request Forgeries: Exploitation and Prevention, TR 2008
- M. Johns, J. Winter, RequestRodeo: client side protection against session riding, OWASP AppSec 2006
- Ph. De Ryck et al., CsFire: Transparent client-side mitigation of malicious cross-domain requests, ESSoS 2010
- A. Barth, C. Jackson, and J. Mitchell, Robust Defenses for Cross-Site Request Forgery, CCS 2008

CsFire – Available now!

- http://distrinet.cs.kuleuven.be/software/CsFire



CsFire 0.7.1

by Philippe De Ryck, Lieven Desmet

CsFire autonomously protects you against dangerous or malicious cross-domain requests, such as Cross-Site Request Forgery (CSRF). CSRF is very prevalent and dangerous, as stated by the OWASP top 10, as well as the CWE/SANS top 25 programming errors.

Updated	June 11, 2010
Website	http://distrinet.cs.kuleuven.be/software/CsFire/
Works with	Firefox: 3.5 - 3.7a5pre
Rating	★★★★★ 6 reviews
Downloads	6,214