UDC 004.056

Roman Bozhok,
Oleksii Aleshchenko

WEB APPLICATION SECURITY

Роман Божок,
Олексій Алещенко

БЕЗПЕКА WEB-ЗАСТОСУНКУ

The article discusses the security issue of a web application. As a research, the site is used. Testing is carried out at the expense of external independent resources.

Key words: OWASP, website, threat, XSS, security.
Fig.: 4. Tabl. 0. Bibl.: 11.

У статті розглядається питання безпеки web-застосунку. В якості дослідження використовується сайт. Тестування виконується за рахунок зовнішніх незалежних ресурсів.

Ключові слова: OWASP, сайт, загроза, XSS, безпека.
Рис.: 4. Табл. 0. Бібл.: 11.

Target setting. The relevance of the security problems of WEB-applications is that they use confidential information, as well as the company's business processes.

Issues analysis. The vast majority of external attacks on corporate information systems are aimed precisely at the vulnerability of web applications.

Actual scientific researches. In recent years, the topic of application security has filled a lot with hype, there are many articles, discussions, and a search for solutions. To solve these problems, an international project on the security of WEB-applications (OWASP) [1] was formed. Problems and their solutions using OWASP are described in more detail in article [2]. Also, in article [3] a certified method is described that will help developers to minimize the occurrence of holes in the program.

Uninvestigated parts of general matters defining. There is no unified protection against all threats and security tools are developing more slowly than methods of application attacks.

The research objective. Investigate the types of threats and check for these threats' web application.

The statement of basic materials. A WEB application is a client-server application, where the client is a browser that displays the user interface, generates

requests to the server, and processes responses from it. And the server part is a WEB-server that processes customer requests. The interaction between the client and the server, as a rule, is carried out via the HTTP protocol [4]. The architecture of WEB applications has three levels [5], which are shown in Figure 1.

Fig. 1. Web application architecture [6]

In connection with the rapid growth of the popularity of information technologies, recommendations have emerged among developers to ensure the security of WEB applications, which resulted in a project called: The Open Web Application Security Project (OWASP).

OWASP is an open source WEB application security project that includes corporations, educational organizations and individual developers who together form articles, recommendations and tutorials that are freely available and recommended when developing WEB applications.

OWASP Top 10 Application Security Risks – 2017 [7]

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization.
- A9:2017-Using Components with Known Vulnerabilities.
- A10:2017-Insufficient Logging and Monitoring.

Experiments. We are exploring the site [8] of the "Department of Computing Engineering", National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" for safety.

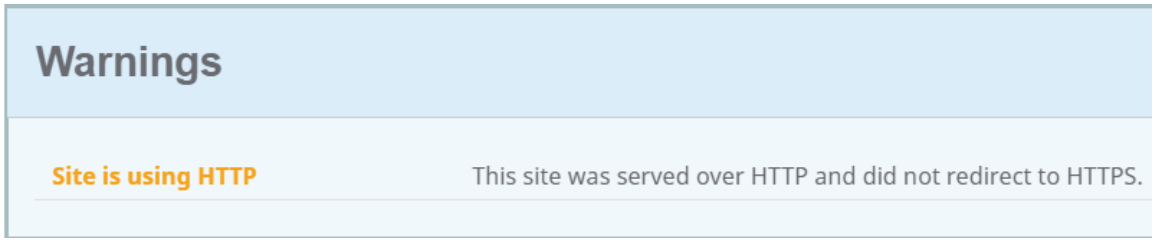

Fig.2. Test from the SecurityHeaders.io service [9]

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud

storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

Redirection	✗	-20	Does not redirect to an HTTPS site
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented

Fig.3. Test from the Observatory by Mozilla service [10]

Redirections. Sites that listen on port 80 should only redirect to the same resource on HTTPS. Once the redirection has occurred, HSTS should ensure that all future attempts go to the site via HTTP are instead sent directly to the secure site.

Referrer Policy. When a user navigates to a site via a hyperlink or a website loads an external resource, browsers inform the destination site of the origin of the requests through the use of the HTTP Referrer (sic) header.

X-Content-Type-Options is a header supported by Internet Explorer, Chrome and Firefox 50+ that tells it not to load scripts and stylesheets unless the server indicates the correct MIME type. Without this header, these browsers can incorrectly detect files as scripts and stylesheets, leading to XSS attacks

X-Frame-Options is an HTTP header that allows sites control over how your site may be framed within an iframe. Clickjacking is a practical attack that allows malicious sites to trick users into clicking links on your site even though they may appear to not be on your site at all.

X-XSS-Protection is a feature of Internet Explorer and Chrome that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.

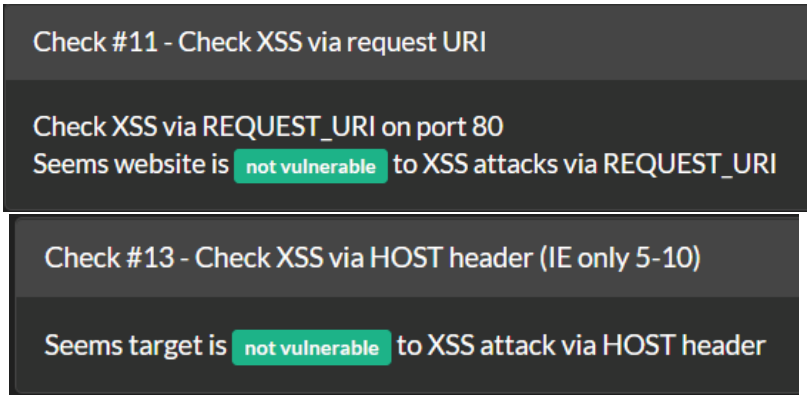

Fig.4. Test from the service One button scan [11]

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Conclusions of experiments. This web application is not properly secure. According to the test results, the average safety rating is “F”.

Conclusions. The article reviewed a list of popular threats. The site of the department was also checked for safety. From the research it is clear that the site is not reliable and needs to be improved. OWASP can help find and fix flaws.

References

1. OWASP. The Open Web Application Security Project. [Електронний ресурс]. — Режим доступу: https://www.owasp.org/index.php/Main_Page

2. БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ. [Електронний ресурс] / Королев О.Л., Лукьянова М.А.// Международная научно-практическая конференция "Проблемы информационной безопасности". — 2016. — №6. — С.166-167. — Режим доступу до журналу: http://ieu.cfuv.ru/sites/default/files/2018-12/sbornik-trudov-2-megd-konf-problemy-inform-bezopasn-2016.pdf#page=166

3. Разработка типовой методики анализа уязвимости в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации. [Електронний ресурс] /Баранов А. В., Федичев А.В. // Вопросы кибербезопасности. — 2016. — №2(15). — С.2-8 — Режим доступу до журналу : https://cyberleninka.ru/article/v/razrabotka-tipovoy-metodiki-analiza-uyazvimostey-v-veb-prilozheniyah-pri-provedenii-sertifikatsionnyh-ispytaniy-po-trebovaniyam

4. Таненбаум Э. Компьютерные сети. Пятое издание / Компьютерные сети. 5-е изд. — СПб.: Питер. — 2012. — С. 724-726

5. Пьюривал С. Основы разработки веб-приложений / С. Пьюривал — СПб.: Питер. — 2015. —272с.

6. ОБЗОР УГРОЗ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ. [Електронний ресурс] / Елисеев Н.А., Федоров С.А., Антонов О.Д. // Вопросы технических наук в свете современных исследований: сб. ст. по матер. V-VI междунар. науч.-практ. конф. — 2018. — № 1(4). — С. 18-23. Режим доступу до журналу: https://sibac.info/conf/technolog y/v/95451

7. OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. [Електронний ресурс]. — Режим доступу: https://www.owasp.org/images/ /7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

8. КАФЕДРА ОБЧИСЛЮВАНОЇ ТЕХНІКИ [Електронний ресурс]. — Режим доступу: http://comsys.kpi.ua/

9. Security Headers [Електронний ресурс]. — Режим доступу: https://securityheaders.com/?q=http%3A%2F%2Fcomsys.kpi.ua%2F&followRedirects=on

10. Mozilla Observatory [Електронний ресурс]. — Режим доступу: https://observatory.mozilla.org/analyze/comsys.kpi.ua

11. Scan #32710 for comsys.kpi.ua from Mon, 29 Apr 2019 21:18:06 +0300 [Електронний ресурс]. — Режим доступу: https://sergeybelove.ru/one-button-scan/result/378e03b41dbeb49d656496b34593c0049728804f/

Autors

Bozhok Roman – bachelor student, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: romabos98@gmail.com

Божок Роман Юрійович – студент III курсу, кафедра обчислюваної техніки, Національний технічний університет України ”Київський політехнічний інститут імені Ігоря Сікорського”.

Aleshchenko Oleksii – senior lecture, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: alexey.aleshchenko@gmail.com

Алещенко Олексій Вадимович – старший викладач, кафедра обчислюваної техніки, Національний технічний університет України ”Київський політехнічний інститут імені Ігоря Сікорського”.

РОЗШИРЕНА АНОТАЦІЯ

Роман Божок,
Олексій Алещенко

БЕЗПЕКА ВЕБ ЗАСТОСУНКУ

Актуальність теми дослідження. Актуальність проблем безпеки веб-застосунків представляється в тому що в них використовується конфіденційна інформація, а також здійснюються бізнес-процеси компанії. Дана робота присвячена захисту та тестуванню саме сайту кафедри, оскільки кожна учбова структура повинна мати добрий захист.

Постановка проблеми. Переважна більшість зовнішніх атак на корпоративні інформаційні системи націлені саме на уразливості веб застосунків.

Аналіз останніх досліджень і публікацій. Протягом останніх років з'являється все більше статей присвячених захисту веб застосунку, зокрема, завдяки появі нових методів був сформований міжнародний проект по забезпеченню безпеки веб застосунків (OWASP). Проте підходи до пошуку відкритих частин для в злому не можливо вивчити досконало так як немає єдиного захисту.

Виділення недосліджених частин загальної проблеми. Дана стаття присвячена вивченню та аналізу запропонованих підходів для пошуку загроз, зокрема на прикладі застосунку одного учбового закладу. Немає єдиного захисту від усіх загроз і безпека не розвивається з великою швидкістю.

Постановка завдання. Завданням є дослідити типи загроз і перевірити ці загрози на веб застосунку.

Викладення основного матеріалу. Проведено аналіз загроз та тестування веб застосунку. Описано рейтинг популярних та актуальних способів в злому сайту. З тестування застосунку видно що він не надійний.

Висновок. Проаналізовано веб застосунок на порядок загроз за допомогою різних незалежних веб ресурсів. Підхід показав себе добре та показав вразливість сайту. Наведені результати експериментів та аналіз загроз.

Ключові слова: OWASP, сайт, загроза, XSS, безпека.